INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Enhancing Business Continuity through Intelligent Process Automation: Governance, Risk Management, and Compliance Frameworks

José Manuel Catarino Barreiros Cascais Brás

PhD in Information Science and Technology

Supervisor(s):
PhD Ruben Filipe Pereira, Assistant Professor,
ISCTE - Instituto Universitário de Lisboa

PhD Sérgio Moro, Full Professor,
ISCTE - Instituto Universitário de Lisboa

June 2024

TECNOLOGIAS
E ARQUITETURA

Department of Information Science and Technology

Enhancing Business Continuity through Intelligent Process Automation: Governance, Risk Management, and Compliance Frameworks

José Manuel Catarino Barreiros Cascais Brás

PhD in Information Science and Technology

Supervisor(s):
PhD Ruben Filipe Pereira, Assistant Professor,
ISCTE - Instituto Universitário de Lisboa

PhD Sérgio Moro, Full Professor,
ISCTE - Instituto Universitário de Lisboa

June 2024

TECNOLOGIAS
E ARQUITETURA

Department of Information Science and Technology

Enhancing Business Continuity through Intelligent Process Automation: Governance, Risk Management, and Compliance Frameworks

José Manuel Catarino Barreiros Cascais Brás

PhD in Information Science and Technology

Jury:
PhD Abílio Gaspar de Oliveira, Associate Professor with Aggregation
ISCTE - Instituto Universitário de Lisboa
PhD José Tribolet, Full Professor
IST - Instituto Superior Técnico
PhD Paulo Guedes, Associate Professor,
ULHT - Universidade Lusófona de Humanidade e Tecnologias
PhD Leandro Pereira, Associate Professor with Habilitation
ISCTE - Instituto Universitário de Lisboa
PhD Ruben Filipe Pereira, Assistant Professor,
ISCTE - Instituto Universitário de Lisboa

June, 2024

“Acredita sempre no que podes alcançar e nunca desistas de tentar, por mais difícil que te pareça”

Carlos Manuel Cascaes Brás

1948 - 1999

Acknowledgments

Completing this thesis has been a long journey, one of my life's most rewarding and challenging projects. It could not have been possible without many individuals' unwavering support, help, and encouragement throughout this time.

First and foremost, I dedicate this work to my daughters and son, Ana, Margarida, and Lourenço Brás, who are my greatest source of inspiration and strength. I extend my deepest thanks to them and offer this message: never give up on what you believe in.

I had the privilege of working with two supervisors on this thesis, Prof. Sérgio Moro, and Prof. Ruben Pereira, and I would like to express my gratitude to both. My special thanks go to Prof. Ruben Pereira for his invaluable guidance, support, and unwavering belief in my work. His expertise and knowledge have been instrumental in bringing this thesis to fruition. I deeply appreciate his patience and availability throughout the work done and for supervising the articles that constitute this thesis.

I also thank my sister Ana and extend special gratitude to my mother, Maria de Lourdes, for her unwavering support, pride, and love, which have been a constant source of motivation. Finally, my deepest thanks go to Anabela for her faith, patience, and endless support.

In addition, I would like to acknowledge and thank COPELABS for their financial support, which was essential to making this research possible. Their investment has significantly contributed to advancing this work, and I am deeply appreciative of their backing throughout this journey. Additionally, I want to express my sincere thanks to my colleague Rui Ribeiro for his invaluable contributions and encouragement during this journey. His support has been instrumental in the completion of this thesis.

To all my friends, with a special mention to Rute Trindade, I extend my gratitude for your support and comprehension throughout this journey. I also want to express my appreciation to all individuals and organizations who contributed to this thesis. Your invaluable involvement made this achievement possible.

Last but not least, I wish to express my heartfelt gratitude to my uncle, Carlos Manuel Cascaes Brás, who has been my primary source of inspiration. His encouragement, when I was young, always pushed me to explore new horizons, such as learning programming, languages like English and Arabic, listening to music, and researching deeper into many other subjects. As a professor, he demonstrated to me the vital importance of supporting his students and imparting the most valuable life lessons - being responsible, well-mannered, and pursuing knowledge. His

unwavering belief in the transformative power of education has profoundly shaped my life journey, and his example has been a guiding light throughout this thesis.

This thesis is dedicated to all of you. Thank you for being a vital part of this remarkable journey.

Resumo

No cenário empresarial contemporâneo, marcado por uma rápida transformação digital e interrupções frequentes, as organizações enfrentam desafios significativos em manter a resiliência operacional. A adoção da Automação Inteligente de Processos (IPA) surgiu como uma estratégia crucial para otimizar processos de forma eficiente. Contudo, a integração da IPA introduz complexidades nos *frameworks* de continuidade de negócios, exigindo estruturas robustas de governança, gestão de riscos e conformidade. Esta tese investiga a integração da IPA nos *frameworks* de Continuidade de Negócios, alinhando essas tecnologias com padrões industriais estabelecidos como IEEE 2755.2:2020 e ISO 22301:2019 para fortalecer as estratégias de continuidade de negócios.

Utilizando uma combinação de metodologias que incluem Revisão de Literatura Multivocal, Pesquisa de Design Científico e entrevistas estruturadas, esta investigação explora os efeitos da IPA na governança, gestão de riscos e capital humano. Oferece um entendimento detalhado de como as organizações podem utilizar a IPA para melhorar a eficiência dos processos enquanto mitigam os riscos associados. O estudo aborda também os desafios únicos de auditoria num ambiente automatizado, especialmente o papel evolutivo dos auditores em garantir a conformidade no setor financeiro. Além disso, examina os riscos específicos introduzidos pela automação e apresenta *insights* sobre *frameworks* eficazes de gestão de riscos que as organizações podem implementar.

Adicionalmente, a tese destaca a importância das estratégias de gestão de mudanças para facilitar a adaptação da força de trabalho à automação, enfatizando a necessidade de iniciativas abrangentes de formação e capacitação. Esta pesquisa avança significativamente na comunicação sobre automação e gestão da continuidade de negócios, unindo tecnologias de automação e práticas de continuidade de negócios. Ela fornece às organizações *frameworks* práticos e estratégias para melhorar a sua resiliência, governança e eficiência operacional num mundo cada vez mais automatizado.

Palavras-chave: Automação de Processos Inteligentes, Robotic Process Automation, Continuidade de Negócios, Governança, Gestão de Riscos, Conformidade.

Abstract

In the contemporary business landscape marked by rapid digital transformation and frequent disruptions, organizations confront significant challenges in maintaining operational resilience. The adoption of Intelligent Process Automation (IPA) has emerged as a pivotal strategy for streamlining processes efficiently. However, IPA's integration introduces complexities into business continuity frameworks, necessitating robust governance, risk management, and compliance (GRC) structures. This thesis delves into the integration of IPA within Business Continuity frameworks, aligning these technologies with established industry standards such as IEEE 2755.2:2020 and ISO 22301:2019 to bolster business continuity strategies.

Utilizing a blend of methodologies including Multivocal Literature Review, Design Science Research, and structured interviews, the research explores the effects of IPA on governance, risk management, and human capital. It offers a detailed understanding of how organizations can utilize IPA to enhance process efficiency while simultaneously mitigating associated risks. The study also addresses the unique auditing challenges within an automated environment, particularly the evolving role of auditors in ensuring compliance within financial sectors. It further scrutinizes the specific risks introduced by automation and provides insights into effective risk management frameworks that organizations can implement.

Additionally, the thesis underscores the importance of change management strategies in facilitating workforce adaptation to automation, highlighting the necessity for comprehensive training and upskilling initiatives. This research significantly advances the discourse on automation and business continuity management, bridging the gap between automation technologies and business continuity practices. It furnishes organizations with practical frameworks and strategies to improve their resilience, governance, and operational efficiency in an increasingly automated world.

Keywords: Intelligent Process Automation, Robotic Process Automation, Business Continuity, Governance, Risk Management, Compliance.

Contents

List of Tables

List of Figures

List of Acronyms

AI	Artificial Intelligent
BC	Business Continuity
BCI	British Standards Institute
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BP	Business Process
BPMS	Business process management systems
CoE	Centre of Excellence
CS	Case Studies
CV	Computer Vision
DORA	Digital Operational Resilience Act
DRP	Disaster Recovery Plan
DSR	Design Science Research
DSRM	Design Science Research Method
DT	Digital technology
ET	Emerging Technologies
GL	Grey Literature
GRC	Governance, Risk, and Compliance
IA	Internal Audit
IAFs	Internal Audit Functions
IAM	Identity and Access Management
ICT	Information, and Communication Technologies
IPA	Intelligent Process Automation
ISO	International Organization for Standardization
IT	Information Technologies
KPI	Key Performance Indicators
ML	Machine Learning
MLR	Multivocal Literature Review
NLP	Natural Language Processing
PDCA	Plan, Do, Check, and Act
PPT	People, Processes, and Technology
RPA	Robotic Process Automation
SBIPA	Software-Based Intelligent Process Automation
SLR	Systematic Literature Review

Chapter 1
Introduction

This chapter offers a comprehensive overview of the entire body of work presented in this thesis. It opens by examining the background and rationale for this research, laying out its context, objectives, purpose, and primary research question.

Subsequently, the chapter shifts its focus to the conceptual framework and research areas that underpin this thesis. This multidisciplinary research project addresses timely and relevant topics, supported by a foundation that includes a Multivocal Literature Review (MLR). This MLR established the motivation and helped shape the areas of inquiry for this thesis, alongside other research activities conducted. However, certain sections are not elaborated upon in depth to avoid redundancy, as the foundational background information is already covered in the published articles that are reflected in this section.

Furthermore, three additional sections have been integrated into this chapter. The first section delineates the various contributions of this thesis, providing further clarity on topics discussed in the published articles. The second section lists all peer-reviewed papers that have been published, along with a comprehensive bibliography of journal publications. Finally, the Chapter 1 concludes by outlining the document's organization, which is critical for readability and understanding of the research flow, considering the article-based thesis structure of this work.

1.1. Context, Problem, and Motivation

The contemporary business environment is marked by rapid technological advancement and unprecedented disruptions, epitomized by global events such as the COVID-19 pandemic [1, 2, 3]. These events have underscored businesses' need to build resilience and adaptability into their operations. This backdrop has amplified the importance of digital transformation, which enables organizations to leverage technology to streamline operations and enhance agility in response to external shocks [4].

Automation technologies, particularly Robotic Process Automation (RPA) and Intelligent Process Automation (IPA) have emerged as critical components in this transformation [5]. RPA refers to the use of software robots to automate repetitive, rule-based tasks, while IPA extends this functionality through artificial intelligence (AI), enabling the automation of more complex processes involving cognitive decision-making and learning capabilities [6]. These

technologies promise to revolutionize how businesses operate by increasing efficiency, reducing human errors, and enabling faster responses to market changes.

As organizations increasingly rely on RPA and IPA to drive their digital strategies, business continuity (BC) management becomes paramount [7]. BC ensures that organizations can continue delivering critical services during and after disruptive incidents. This requires comprehensive planning that considers potential threats, develops robust response strategies, and incorporates technologies that enable resilience [8].

However, integrating RPA and IPA into business continuity management (BCM) introduces a set of challenges. Automation, while beneficial, can amplify risks if not managed properly. These risks include the potential for automation failures to interrupt critical processes, challenges in maintaining governance over increasingly automated workflows, and the need to align automated systems with evolving regulatory frameworks [9, 10, 11, 12].

The need for comprehensive research on the interplay between RPA, IPA, and BC is highlighted by Brás et al. (2023) [8]. Their work emphasizes the importance of understanding how these technologies can be harnessed to bolster BC while also acknowledging the gaps in current knowledge. The need to explore how automation technologies impact BC planning and execution becomes imperative as more organizations adopt these tools to transform their operations [7, 8].

Given this context, businesses must approach the integration of RPA and IPA into their BC strategies with caution, ensuring they understand the potential pitfalls and establish frameworks to manage the risks. The dynamic nature of today's business landscape makes it vital to have adaptive strategies that can evolve alongside technological advancements and shifting regulatory environments [13, 14, 15, 16].

1.2. Problem Definition

The integration of RPA and IPA into business processes presents significant opportunities for efficiency and innovation but also introduces complexities that can impact BCM [17, 18]. While RPA and IPA can automate repetitive tasks, optimize workflows, and reduce costs, their implementation within organizations poses challenges that need to be addressed systematically. Below are some of the most critical issues related to the implementation of these technologies:

Operational Risks and Failures:

The automation of critical business processes through RPA and IPA increases dependence on these technologies for continuity. This dependency creates operational risks, particularly if the automation fails. Such failures can result from software bugs, misconfigurations, or

incompatibilities with updated systems. These disruptions can have significant consequences, particularly when organizations lack robust fallback mechanisms or have not comprehensively assessed the potential impact of automation failures [19, 20, 21].

Governance and Oversight:

Integrating RPA and IPA into an organization's processes necessitates establishing new governance structures to manage these technologies effectively. This includes defining clear policies and procedures that outline the acceptable use of automation, risk management practices, and response strategies. Without robust governance frameworks, organizations risk losing control over their automated workflows, leading to inefficiencies, security vulnerabilities, and non-compliance with regulatory standards [22, 23, 24, 25].

Security and Compliance Challenges:

Automated processes can inadvertently introduce security vulnerabilities, particularly when they interact with sensitive data or connect with external systems. RPA and IPA can increase exposure to cyber threats if not properly secured. Additionally, organizations must ensure compliance with relevant regulations, which may vary across industries and regions. The lack of standardization in how RPA and IPA tools handle data can further complicate compliance efforts, potentially exposing organizations to regulatory penalties [24, 26].

Integration with Existing BC Plans:

Traditional business continuity plans may not fully account for the unique challenges introduced by automation. For instance, RPA and IPA can change the nature of critical dependencies within workflows, necessitating updates to existing recovery strategies. Moreover, automation can introduce new points of failure that need to be incorporated into BC plans. This requires organizations to reevaluate their existing BC frameworks and adapt them to account for the nuances of automation [7].

Human Capital and Process Changes:

The shift toward automated processes impacts the workforce by redefining roles and requiring new skill sets. This transition can lead to resistance or challenges in adoption, which may undermine the effectiveness of automation. Additionally, the processes themselves may need to be restructured to accommodate automation, which can disrupt established workflows and require significant change management efforts [27].

Lack of Comprehensive Research and Guidelines:

Despite the growing interest in RPA and IPA, there is a paucity of comprehensive research that provides clear guidelines on effectively integrating these technologies into business continuity strategies. Brás et al. (2023) highlight the gaps in understanding the impact of RPA and IPA

on BC and the need for further research to guide organizations in managing these challenges [8] .

Addressing these problems requires a holistic approach that includes thorough planning, stakeholder engagement, and continuous monitoring. This research seeks to address the gaps in understanding and provide actionable insights for effectively integrating RPA and IPA into business continuity planning.

The motivation for this thesis stems from the urgent need to understand and address the complexities that arise when integrating automation technologies such as RPA and IPA into BC frameworks [28, 29]. The rapid advancement of digital transformation and the adoption of automation technologies have left many organizations without clear guidance on how to align these technologies with their BC strategies effectively [30, 31, 32].

To effectively understand the complexities involved in integrating RPA and IPA into BC strategies, several critical areas warrant detailed exploration. These include the disruptions automation may introduce, the governance frameworks necessary for efficient management, the challenges surrounding security and compliance, the imperative to integrate automation into current BC plans, the implications for human capital and process changes, and the dearth of comprehensive research and guidelines in this domain [7]. The following topics will provide an overview examination of each of these areas:

- **Increasing Adoption of Automation Technologies**

  Organizations are increasingly adopting RPA and IPA to streamline their operations and drive efficiencies [33]. These technologies promise to revolutionize business processes, but their widespread adoption introduces new challenges that organizations are not fully prepared to manage. The complexities of integrating automation into BC strategies necessitate a comprehensive framework that can guide organizations through this process [34].

- **Heightened Risk Environment**

  The global business environment is becoming increasingly volatile, with disruptions ranging from pandemics to cyber-attacks. In such a landscape, maintaining business continuity is paramount. Automation technologies can help address some of these challenges by improving operational resilience, but only if they are correctly integrated into BC plans. Understanding how RPA and IPA affect organizational risk profiles is essential for ensuring that these technologies enhance rather than compromise BC [17, 35, 36, 37].

- **Gaps in Research and Industry Guidance**

  Despite the growing interest in RPA and IPA, there is a lack of comprehensive research that provides clear guidance on effectively integrating these technologies into BC strategies. Most existing literature focuses on the operational benefits of automation without delving into its implications for business continuity. Brás et al. (2023) highlight the need for more targeted research that examines the intersection of automation and BC to provide actionable insights [8].

- **Evolving Compliance and Regulatory Requirements**

  As organizations adopt more sophisticated automation technologies, they must navigate an evolving landscape of compliance and regulatory requirements. These requirements vary by industry and region and often lack clear guidance on how to apply automation technologies while remaining compliant [38, 39, 40]. This lack of clarity creates uncertainty and necessitates a framework that organizations can use to navigate compliance issues related to RPA and IPA in the context of BC [7].

- **Changing Workforce Dynamics**

  Automation is reshaping workforce dynamics, redefining roles, and requiring new skill sets. This shift necessitates change management efforts to help employees adapt to new roles while ensuring that automated processes are effectively managed. There is a need for research that examines how to best align human capital strategies with automation and BC requirements, ensuring that organizations can leverage the full potential of their workforce in this new landscape [27, 41].

- **Strategic Imperative for Business Leaders**

  For business leaders, the ability to maintain continuity in operations while embracing digital transformation is a strategic imperative. Integrating RPA and IPA into BC frameworks is no longer optional but necessary for staying competitive. Business leaders need practical guidance on how to incorporate automation technologies into their continuity plans, ensuring that these technologies deliver value without compromising resilience [1, 42, 43, 44, 45, 46].

In summary, this thesis is motivated by the critical need to provide organizations with a framework for effectively integrating RPA and IPA into BC strategies. By addressing research gaps, offering practical guidance, and highlighting the strategic importance of automation in business continuity, this work aims to help organizations navigate the complexities of digital transformation in an increasingly uncertain world.

The rapid adoption of RPA and IPA in business operations presents new challenges for ensuring BC. Organizations face difficulties in integrating these automation technologies into their BC frameworks due to a lack of clear guidelines, governance issues, evolving risks, workforce adaptation challenges, and audit complexities. This gap necessitates a comprehensive understanding of the interplay between RPA/IPA and BC to develop effective strategies that ensure resilience, manage risks, and support robust audit and governance practices.

Thus, Figure 1.1 encapsulates this thesis's core challenge and guiding question: *How can RPA and IPA be effectively integrated into business continuity management?* This inquiry seeks to develop frameworks and best practices to address the critical areas of governance, risk management, auditing, and workforce adaptation, all at the same time, ensuring compliance and operational resilience are maintained.

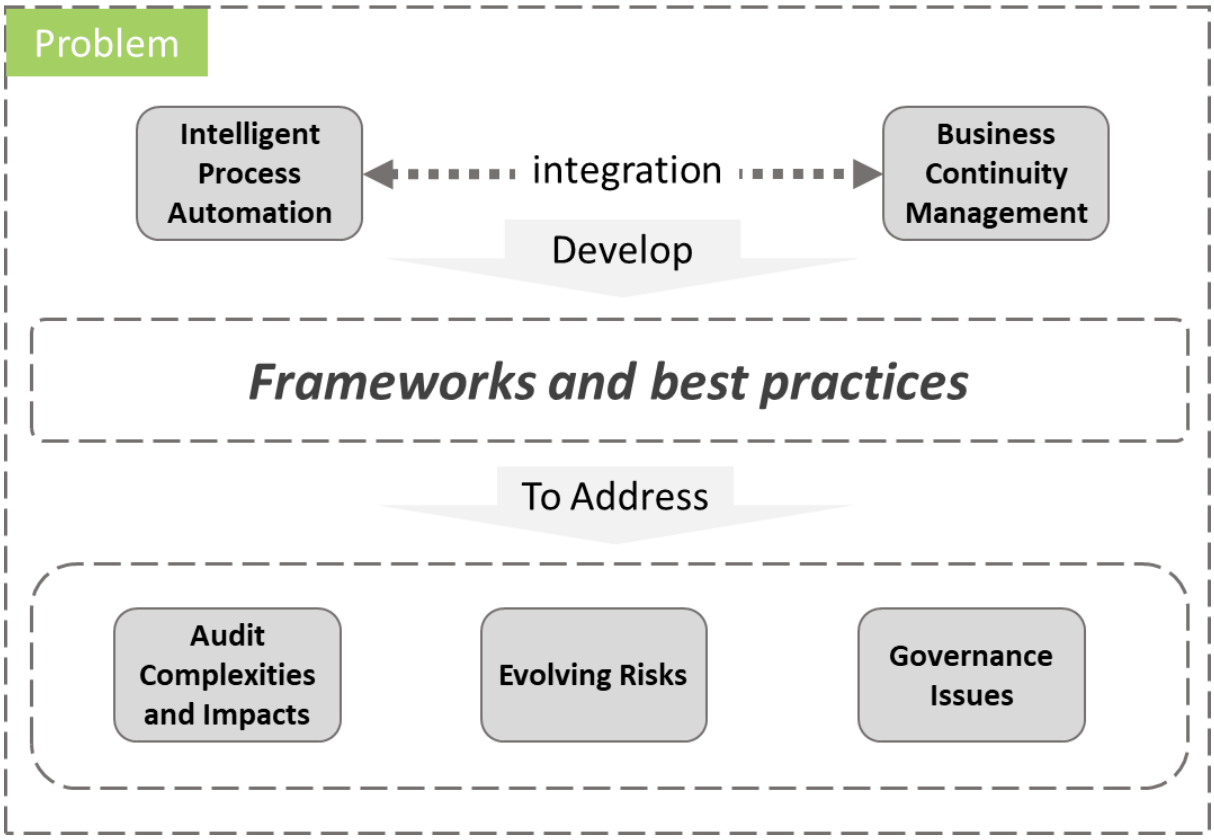


Figure 1.1 - Research Problem Overview: Integration of IPA into BCM.

During this thesis, an MLR was conducted to comprehensively address the research question and meet the research objectives. The research aims to understand how RPA and IPA intersect with business continuity, identifying key areas of alignment and addressing gaps in the current understanding.

In the evolving landscape of business continuity, the interplay between People, Processes, and Technology (PPT), Governance, Risk, and Compliance (GRC), RPA, and IPA with the IEEE

2755:2020 standard [47], and Business Continuity guided by ISO 22301:2019 [48], form the core pillars of this thesis, expressed in Figure 1.2. Effective automation implementation relies heavily on the harmonization of PPT, where people drive change, processes are redesigned to align with business continuity strategies, and technology provides the necessary tools for optimization. GRC frameworks ensure that automation initiatives align with organizational objectives while managing the risks and compliance challenges that arise. The IEEE 2755:2020 standard offers a structured approach to deploying intelligent process automation, emphasizing governance and risk management to maintain operational resilience. The ISO 22301:2019 standard complements this by outlining robust business continuity frameworks that help organizations prepare for, respond to, and recover from disruptions. Together, these four domains create a comprehensive framework for integrating automation into business continuity strategies, enabling organizations to harness the transformative power of RPA and IPA while maintaining operational resilience.

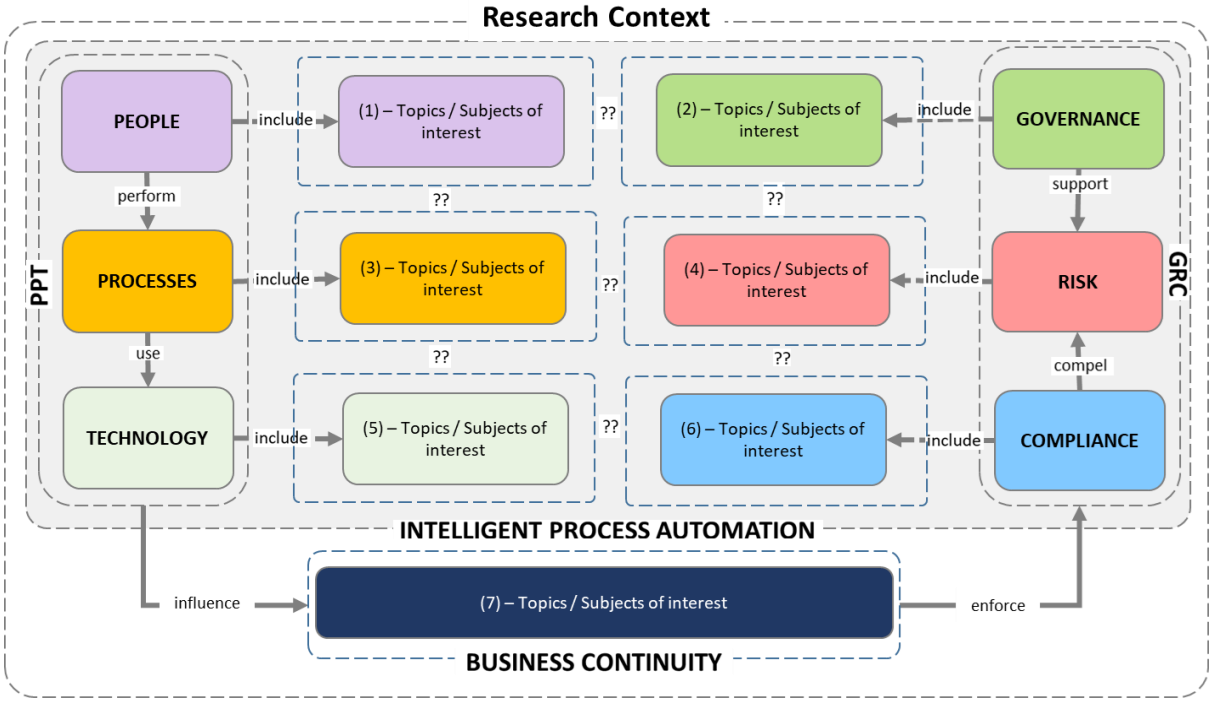


Figure 1.2 - Research context for IPA and BC.

During this process, the investigation produced four research articles that further explored specific topics in this field.

The research conducted within this thesis offers a multifaceted exploration of how automation technologies, specifically RPA and IPA, intersect with BC [7]. The studies collectively highlight the significance of aligning automation practices with established BC frameworks to enhance organizational resilience. By mapping the relationship between standards, and

between topics, the research provides a framework for organizations to integrate intelligent process automation in a way that aligns with BC management objectives.

Additionally, this study emphasizes the role of auditing in maintaining business continuity, especially in sectors such as finance, where the adoption of automation technologies can redefine traditional practices. It also analyses the risks that automation introduces into business processes and offers insights for mitigating potential disruptions. Finally, the research examines the governance and human capital dynamics of RPA integration, emphasizing the need for organizations to effectively balance technology with human resources. Together, these insights offer a comprehensive understanding of the challenges and opportunities that arise from the integration of automation technologies with business continuity.

1.3. Background

As previously introduced, the work developed within the scope of this thesis focuses on four research areas: PPT, GRC, IPA, and BC. Hence, this section offers an overview of these concepts, highlighting the interconnected theories that have shaped and influenced their development [6, 49, 50]. Its purpose is to establish a theoretical foundation, enabling the subsequent chapters to present their discussions and analyses with greater clarity and precision. The integration of automation technologies like RPA and IPA within organizations hinges on a delicate balance between three fundamental components: people, processes, and technology. Each of these components plays a crucial role in ensuring that the adoption of automation technologies is not only successful but also sustainable in the long term.

People, Processes, and Technology (PPT)

The integration of automation technologies like RPA and IPA in organizations hinges significantly on the interplay between people, processes, and technology. People are at the core of any successful implementation, driving the change required for automation adoption while adapting to new workflows. The process component focuses on the redesign of existing workflows to accommodate automation, which involves mapping out tasks suitable for automation and establishing new processes that align with business continuity strategies. Technology, the enabler of this transformation, provides the necessary tools to optimize and enhance these processes. The study by Brás et al. (2023) highlights the need for harmonizing these three elements to fully leverage the potential of automation, emphasizing that technology alone cannot drive change without the proper alignment of people and processes [8].

People

People form the bedrock of any successful automation initiative. They are not only the end-users of these technologies but also the drivers of change within the organization. For RPA and IPA adoption to be successful, there must be a cultural shift that embraces automation as a means to enhance efficiency and productivity. This involves training employees to work alongside automated systems, helping them to understand how automation will impact their roles, and guiding them through the transition. Effective change management is essential to address resistance and ensure that employees are equipped with the skills necessary to leverage automation tools fully [27, 41].

Processes:

The process component involves re-engineering existing workflows to accommodate automation, which is not a trivial task [51, 52, 53]. Organizations must carefully assess which tasks are suitable for automation and how to integrate automated workflows into existing processes [54]. This requires a deep understanding of the organization's operational structure and business continuity strategies. Mapping out processes to identify automation opportunities ensures that RPA and IPA are implemented in areas where they can deliver the most value without disrupting critical workflows. Moreover, the implementation of automated processes should align with the broader goals of business continuity, ensuring that the organization can maintain operations even during disruptions [7].

Technology

Technology is the enabler that drives the transformation in automation. It provides the tools and platforms that organizations use to automate processes, whether through simple task automation with RPA or more complex workflows with IPA. The selection of technology should align with the organization's needs and be scalable to accommodate future growth. However, technology alone is not sufficient to drive change. Without a proper alignment of people and processes, even the most advanced technology can fail to deliver its intended benefits [5].

Brás et al. (2023) emphasize that the full potential of automation can only be realized through the harmonization of these three elements. Technology should be leveraged to optimize processes, but this requires the right people to manage and adapt to the change. It is this alignment of people, processes, and technology that allows organizations to navigate the complexities of automation and derive sustainable value from their RPA and IPA investments [8].

Governance, Risk, and Compliance (GRC)

Governance, Risk, and Compliance form a critical framework for managing RPA and IPA within the context of business continuity. Governance ensures that automation initiatives align with the organization's overall objectives and that clear policies guide implementation. Risk management identifies and mitigates potential disruptions that automation could introduce into critical business processes. Compliance ensures that these initiatives adhere to industry standards, regulations, and internal policies. The integration of automation technologies into BC requires robust governance structures to manage the risks and compliance challenges effectively. By providing a framework for assessing and mitigating risks, organizations can ensure their automation initiatives do not compromise their ability to recover from disruptions. GRC forms a foundational framework for effectively managing RPA and IPA within the context of business continuity. Governance plays a pivotal role by setting the strategic direction for automation initiatives, ensuring they are in alignment with the organization's broader goals and objectives. This requires the establishment of clear policies and procedures that provide a structured approach to implementing automation across various business processes. Strong governance also includes the formation of steering committees and cross-functional teams that provide oversight, ensuring that RPA and IPA initiatives remain aligned with BC objectives and adapt to changes in the business environment [32].

Risk management focuses on identifying, assessing, and mitigating the potential disruptions that automation could introduce into business processes. This involves conducting thorough risk assessments to identify vulnerabilities in automated workflows and developing strategies to mitigate those risks. For instance, organizations must consider how automation impacts cybersecurity, data integrity, and system availability. Effective risk management ensures that automated systems have built-in redundancies and safeguards to maintain business continuity even in the event of an automation failure [21, 55].

Compliance, the third pillar, is crucial in ensuring that automation initiatives adhere to both external regulations and internal policies. This includes adhering to industry standards, such as those set by ISO and IEEE, as well as regional regulatory requirements. Compliance also extends to internal governance policies that define how automated systems should be used and monitored. With the rapid evolution of regulatory landscapes, particularly in data privacy and cybersecurity, compliance teams must remain agile and ensure that automation initiatives are always in line with current regulations.

The integration of automation technologies into BC frameworks necessitates robust GRC structures to effectively manage the associated risks and compliance challenges. Organizations

that adopt a comprehensive GRC approach can more accurately assess the potential impacts of automation on their BC strategies, ensuring that they do not compromise their ability to respond to disruptions. By establishing a framework that combines governance oversight, risk assessment, and compliance monitoring, organizations can navigate the complexities of automation in a way that enhances their resilience and operational efficiency [17].

RPA/IPA with IEEE 2755:2020

The IEEE 2755:2020 standard offers a comprehensive framework that is vital for implementing and managing intelligent process automation systems like RPA and IPA [47]. It establishes detailed guidelines encompassing system architecture, data management, security, performance, and more. By following these guidelines, organizations can ensure that their automation initiatives are not only well-designed but also managed effectively, promoting both efficiency and compliance in their operations.

System architecture plays a crucial role in ensuring that automated processes integrate seamlessly into existing IT infrastructure while maintaining the flexibility needed for future upgrades. By adhering to IEEE 2755:2020 guidelines on architecture, organizations can create scalable and robust automation systems that align with broader IT strategies and business continuity needs.

Data management, another critical area addressed by the standard, involves handling vast amounts of data generated by automated systems. Proper management ensures that data is collected, stored, and analysed securely and efficiently, supporting automation's decision-making capabilities without compromising data integrity. Security guidelines in the standard help protect automated processes from vulnerabilities and threats that could compromise business continuity [28, 56, 57].

Performance is a key aspect of IEEE 2755:2020, providing metrics and benchmarks that organizations can use to gauge the effectiveness of their automation systems. These benchmarks help in continuously improving the automation processes, ensuring that they meet the desired performance levels and align with business objectives.

Aligning RPA and IPA practices with the IEEE 2755:2020 standard also facilitates seamless integration into existing business continuity frameworks. This alignment ensures that automation initiatives bolster operational resilience by supporting critical business functions even during disruptions. The standard's focus on governance and management methodologies guides organizations in deploying automation systems in a way that enhances resilience, ensuring that these systems can adapt to changing business environments and requirements.

In essence, IEEE 2755:2020 serves as a cornerstone for organizations aiming to integrate RPA and IPA into their operations, offering structured guidance that encompasses all facets of automation implementation. By adhering to this standard, organizations can fully leverage the potential of automation while safeguarding against risks and ensuring consistent, reliable performance in support of business continuity.

Business Continuity with ISO 22301:2019

ISO 22301:2019 is a globally recognized standard that provides a comprehensive framework for establishing, implementing, maintaining, and enhancing business continuity management systems (BCMS) [48]. It is crucial to help organizations ensure they can continue delivering critical services during and after disruptive incidents, thereby safeguarding their resilience and sustainability. The standard lays out a systematic approach to developing BCMS that identifies potential threats, assesses their impacts, and formulates robust response strategies that keep critical business functions operational [58].

To effectively integrate RPA and IPA into BC frameworks, organizations must align these automation technologies with the principles of ISO 22301:2019 [7]. This requires embedding automation practices within the broader BCMS, ensuring that automation not only complements but also enhances business continuity. Key to this alignment is understanding the specific risks and challenges posed by automation, such as technology failures, cybersecurity threats, and process disruptions, and incorporating them into BC planning and strategies [59, 60].

The standard emphasizes risk-based thinking, which is essential in evaluating how automation affects business continuity. By identifying and mitigating automation-related risks, organizations can ensure that their automated processes do not become single points of failure in the event of a disruption. The ISO 22301:2019 standard also stresses the importance of clear communication and incident response planning, which must include automated processes to ensure seamless recovery.

Furthermore, mapping the relationship between ISO 22301:2019 and the IEEE 2755.2:2020 standard provides a framework that guides organizations in aligning their automation initiatives with business continuity standards. This mapping offers a holistic view of how intelligent automation can be leveraged to enhance BC strategies while ensuring that technology deployments adhere to established principles of resilience [7]. The research demonstrates how to integrate these standards, enabling organizations to create a cohesive strategy that incorporates automation into BC plans, thereby ensuring the continuity of critical operations.

Ultimately, ISO 22301:2019 provides a structured methodology that organizations can use to align their automation initiatives with BC objectives, reinforcing their resilience efforts [61, 62, 63, 64, 65]. By embedding RPA and IPA into BCMS, organizations can streamline their response to disruptions, reduce downtime, and maintain the continuity of critical services, all while leveraging the efficiency and speed of automation.

1.4. Contributions

Given the objective of this thesis, the primary expected contributions lie in the theoretical exploration of integrating RPA and IPA within the context of BC. This research offers substantial contributions to both academic discourse and practical applications. Through a thorough analysis of existing frameworks and industry practices, this research provides valuable insights into the alignment of automation technologies with BC strategies. By mapping the relationship between IEEE 2755.2:2020 and ISO 22301:2019 standards, the thesis establishes a structured approach to embedding process automation within BC management systems. This approach ensures that organizations can optimize their automation initiatives while maintaining resilience against disruptions.

The research specifically targets the banking sector due to its critical role in the financial ecosystem and its high regulatory demands. This sector is uniquely impacted by automation because of the stringent compliance requirements and the significant volume of transactions processed, which demand precision and accountability. Therefore, one of the studies focuses on how automation technologies, particularly in auditing practices within banks, can uphold and enhance regulatory compliance and operational integrity. This approach not only addresses the sector-specific challenges but also provides valuable insights that apply to other areas of the financial industry. The article on auditing in the banking sector thus serves as a pivotal component of the research, illustrating practical implementations and the tangible benefits of integrating RPA and IPA into existing auditing frameworks in a highly regulated environment. The work offers a comprehensive exploration of how auditing practices can adapt to the challenges presented by automation. It emphasizes the importance of maintaining rigorous standards to ensure that BC is not compromised in highly regulated environments. By examining the evolving role of auditors in an automated landscape, the research contributes to the development of best practices for integrating automation into existing auditing frameworks [66].

Addressing the risks posed by RPA and IPA, the thesis provides a framework for identifying and mitigating disruptions in automated processes. The analysis delves into the challenges that automation introduces to critical business functions, offering practical guidelines for organizations to assess and manage these risks effectively. By highlighting the potential vulnerabilities of

automation systems, the research advocates for a proactive approach to risk management that supports uninterrupted business operations.

Additionally, the thesis explores the governance and human capital dynamics of RPA and IPA integration. It emphasizes the need for a balanced approach that considers the interplay between technology and human resources. The research presents strategies for ensuring successful RPA adoption while maintaining BC, addressing the complexities of change management, workforce adaptation, and governance. This holistic perspective on automation integration offers actionable insights for organizations seeking to maximize the benefits of automation while ensuring that governance and workforce challenges are effectively managed.

In summary, the thesis provides a comprehensive framework for understanding and addressing the challenges and opportunities that arise from integrating automation technologies into business continuity strategies. Its findings significantly contribute to the fields of BC, auditing, risk management, and governance, offering actionable insights for practitioners and advancing academic discourse in these areas.

1.5. List of publications

In the development of this thesis, rigorous original research was conducted, holding distinctive merit and demonstrating its capacity for independent publication. The primary objective was to ensure that our research subjects made a significant impact on the field, underwent rigorous peer review, and attained scientific recognition by being published in reputable journals. This objective was realized through a meticulous approach to the research problem that permeated the entire thesis development process.

It is imperative to highlight that the thesis team assumed comprehensive responsibility for all published papers. The PhD candidate, as the primary author, played a pivotal role in leading the research, while the co-authors provided indispensable support through consistent mentoring and critical supervisory contributions. The accepted articles and submitted articles, along with details about the journals where they were published, are presented below in Figure 1.3. It was employed the SCImago Journal Rank (SJR) to populate the data depicted in Figure 1.3. The SJR indicator is utilized to measure the scientific influence of academic journals. It considers not only the number of citations a journal receives but also the prestige of the journals from which these citations originate. This dual consideration is critical for accurately gauging a journal's influence and prestige.

If scientific impact is related to the number of endorsements a journal receives in the form of citations, then prestige can be understood as a combination of both the number of endorsements and the prestige or importance of the journals issuing these citations. The SJR indicator assigns

different values to citations based on the importance of the journals they come from. Thus, citations from highly prestigious journals are more valuable and, consequently, confer more prestige on the journals that receive them. The calculation of the SJR indicator is similar to the Eigenfactor score. However, SJR is based on the Scopus database, while the Eigenfactor score relies on the Web of Science database. The image highlights various research areas, such as Business Continuity and Intelligent Process Automation, and showcases journals with their corresponding SJR values, which reflect their scientific impact and prestige within their respective fields.

This nuanced approach to evaluating journal influence underscores the importance of considering both citation counts and the prestige of citing journals, providing a more comprehensive measure of a journal's scientific impact. The recommended citations for these articles are as follows:

Published Articles:

1. J. Brás, R. Pereira, and S. Moro, ‘‘Intelligent process automation and business continuity: Areas for future research,’’ Information, vol. 14, no. 2, p. 122, Feb. 2023, doi: 10.3390/info14020122.
   Impact Score: 3.1

2. J. Cascais Brás, R. F. Pereira, S. Moro, I. S. Bianchi and R. Ribeiro, "Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019," in IEEE Access, vol. 11, pp. 134239-134258, 2023, doi: 10.1109/ACCESS.2023.3337159.
   Impact Score: 3.9

3. José Cascais Brás, Ruben Filipe Pereira, Micaela Fonseca, Rui Ribeiro, Isaias Scalabrin Bianchi, “Advances in Auditing and Business Continuity: A Study in Financial Companies”, in Journal of Open Innovation: Technology, Market, and Complexity, 2024, 100304, ISSN 2199-8531, https://doi.org/10.1016/j.joitmc.2024.100304.
   Impact Score: 4.3

Submitted Articles:

4. Title: "Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective."

   Authors: José Cascais Brás, Ruben Pereira, Isaias Scalabrin Bianchi, Pedro Brites, Rui Ribeiro.

   Journal: Schmalenbach Journal of Business Research

   Submission Date: 04/29/2023

   Impact Score: 11.3

5. Title: "Balancing Business, IT, and Human Capital: RPA Integration and Governance Dynamics."
   Authors: José Cascais Brás, Ruben Pereira, Marcela Mello, Sérgio Moro, Isaias Scalabrin Bianchi.
   Journal: SAGE Open
   Submission Date: 03/05/2023
   Impact Score: 2.0

1.6. Thesis research design

Figure 1.4 illustrates the result of the first article, the centrepiece of the figure, which was a result of the initial research that ended up shaping the fundamental structure of the thesis, portraying the interconnected nature of the articles that make up the body of the research. The first article sets the stage by establishing the motivation and fundamental areas for research that underpin the thesis. The subsequent articles build on this foundation, linking key aspects of Intelligent Process Automation with governance, risk management, and compliance. Each article addresses distinct yet overlapping areas within the thematic clusters of technology, business continuity, and compliance, contributing to a comprehensive understanding of the impact of automation in organizational settings. This visual representation emphasizes the progression and integration of topics that collectively enhance the robustness of business continuity strategies through the application of governance and risk management frameworks. The articles are structured to progressively build upon each other, elaborating on the nuances of automation within the framework of established business continuity and governance structures. For example, one article might explore the technical implementations of automation, while another examines the implications of these technologies on compliance and risk management. This layered approach allows the thesis to cover the subject matter comprehensively, addressing both the micro-level details and their macro-level implications on business strategies.

Moreover, the visual representation in the diagram highlights the methodical progression and integration of these topics, illustrating how they collectively contribute to strengthening business continuity strategies. By mapping out the connections between the articles and the core themes they explore, the diagram emphasizes the strategic alignment of governance and risk management frameworks with technological advancements in automation. This not only reinforces the thesis's argument about the benefits of Intelligent Process Automation but also underscores the importance of a well-coordinated approach in managing the complexities introduced by these technologies.

The research approach adopted in this thesis is both systematic and iterative, ensuring each article not only stands on its own merit but also seamlessly connects with the others to form a comprehensive narrative. The methodical planning and execution of this research demonstrate a thorough academic approach that provides valuable insights into integrating cutting-edge technologies within traditional business frameworks. This study aims to enhance operational efficiency and resilience, addressing the challenges posed by digital transformation.

PhD Thesis

MOTIVATION

Publication date:
02/14/2023
Cited by:
5
Impact Score:
3.1

Intelligent Process Automation and Business Continuity: Areas for Future Research

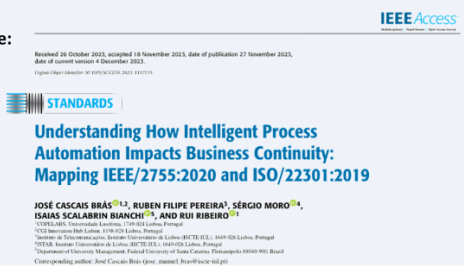
José Cascais Brás
University Institute of Lisbon, Portugal
Jose_manuel_bras@iscte-iul.pt
Ruben Pereira
University Institute of Lisbon, Portugal
Sérgio Moro
University Institute of Lisbon, Portugal

RESEARCH AREAS

Survey Research

Business Continuity and Intelligent Process Automation

Publication date:
11/27/2023
Cited by:
1
Impact Score:
3.9



Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019

JOSÉ CASCAIS BRÁS, RUBEN FILIPE PEREIRA, SÉRGIO MORO, ISAIAS SCALABRIN BIANCHI, AND RUI RIBEIRO

Multivocal Literature Review

Audit

Publication date:
05/16/2024
Cited by:
0
Impact Score:
4.3

Advances in Auditing and Business Continuity: A Study in Financial Companies

José Cascais Brás
University Institute of Lisbon, Portugal
Jose_manuel_bras@iscte-iul.pt
Ruben Pereira
University Institute of Lisbon, Portugal
Isaias Scalabrin Bianchi
Federal University of Santa Catarina, Brazil
Micaela Freitas da Fonseca
University Institute of Lisbon, Portugal
Rui Ribeiro
Lusófona University, Portugal

Multivocal Literature Review

Risk

Submission date:
04/29/2024
Cited by:
0
Impact Score:
11.3

Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective

José Cascais Brás
University Institute of Lisbon, Portugal
Jose_manuel_bras@iscte-iul.pt
Ruben Pereira
University Institute of Lisbon, Portugal
Isaias Scalabrin Bianchi
Federal University of Santa Catarina, Brazil
António Pedro Brites
University Institute of Lisbon, Portugal
Rui Ribeiro
Lusófona University, Portugal

Multivocal Literature Review

People and Governance

Submission date:
03/05/2024
Cited by:
0
Impact Score:
2.0

Balancing Business, IT, and Human Capital: RPA Integration and Governance Dynamics

José Cascais Brás
University Institute of Lisbon, Portugal
Jose_manuel_bras@iscte-iul.pt
Ruben Pereira
University Institute of Lisbon, Portugal
Marcela Mello
University Institute of Lisbon, Portugal
Sérgio Moro
University Institute of Lisbon, Portugal
Isaias Scalabrin Bianchi
Federal University of Santa Catarina, Brazil

Figure 1.3 - Publications list.

1.7. Thesis organization

This thesis adopts an article-based format, allowing for focused contributions to scientific literature while aligning with the overarching goals of the research. The arrangement supports the efficient dissemination of high-quality material for reputable journals, as detailed in Section 1.4 and subsequent chapters.

Chapter 1: Introduction

The introductory chapter outlines the research theme and proposal, providing essential concepts that support subsequent chapters. It also lists the publications included in this thesis and offers a structural overview of the work.

Chapters 2 to 4: Published Articles

Each of these chapters is devoted to a published article that comprises part of this thesis. Per journal standards, each article is formatted as an independent document, complete with its sections, abstracts, references, and pagination. Despite this independence, each article directly contributes to the overarching objectives of the thesis. The chapters are organized chronologically by publication date, as illustrated in Figure 1.3.

Chapters 5 to 6: Submitted Articles

Chapters 5 through 6 are dedicated to articles that have been submitted for peer review and are integral to this thesis. Each article is presented as a distinct entity, adhering to the standard format required by academic journals, which includes individual sections, abstracts, references, and pagination. Although each article stands on its own, it significantly supports the cumulative goals of this thesis. The arrangement of these chapters follows the chronological order of their submission, as depicted in Figure 1.3.

Chapter 7: Conclusion

The concluding chapter synthesizes the main research findings, summarizing the key insights gained from the published articles. It provides a comprehensive thesis summary, drawing overarching conclusions and offering final remarks, limitations, and suggestions for future research.

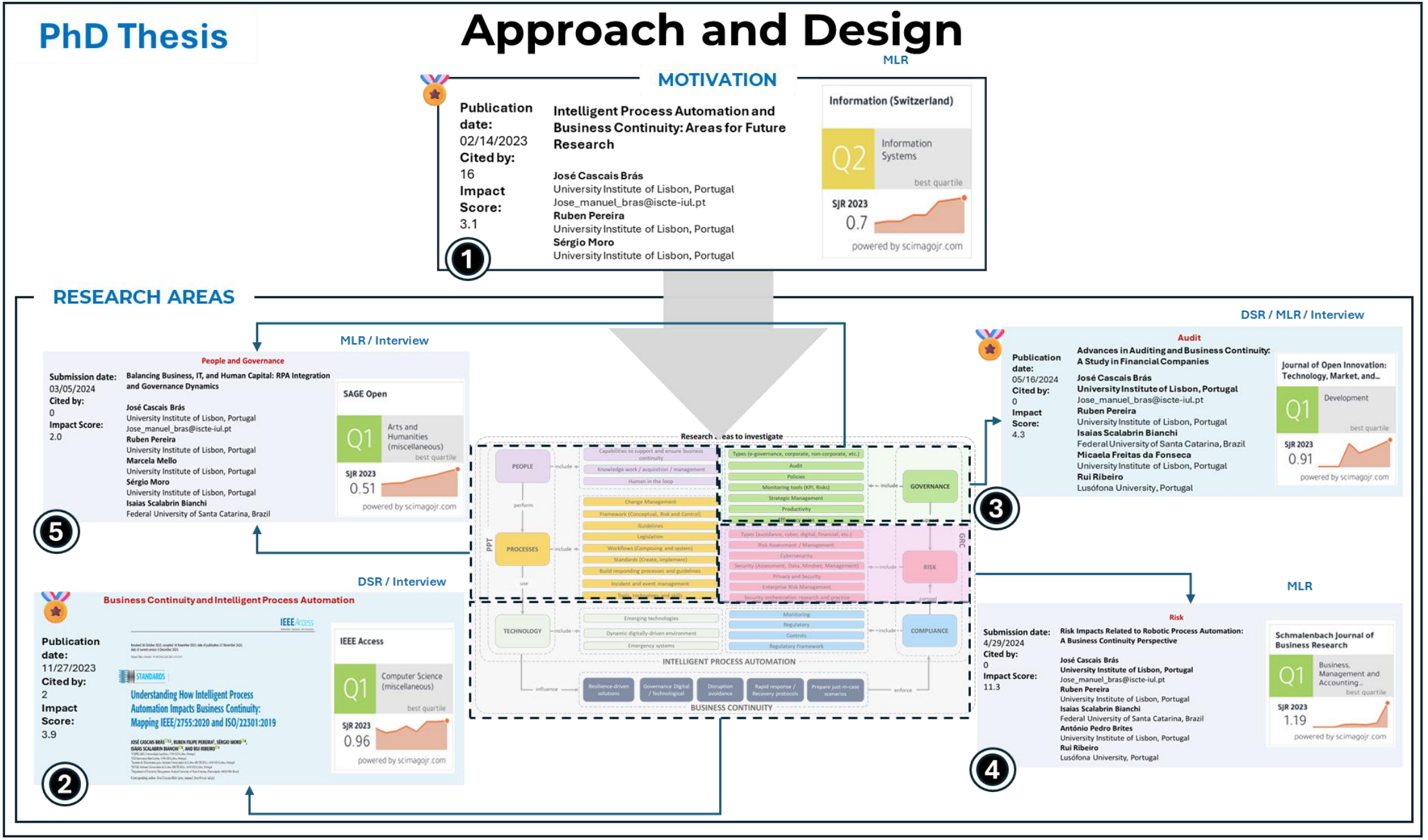


Figure 1.4 - Thesis research design

Chapter 2

Article nr. #1 – "Intelligent Process Automation and Business Continuity: Areas for Future Research"

This article forms the basis and motivation for this thesis. The research presented in this article served as a crucial foundation, having been developed and expanded during the thesis process, thereby fitting within its scope. The study aimed to identify the areas most critical for future research by exploring the intersection of RPA and IPA with BC. It conducted a thorough review of current literature and industry reports, revealing gaps in understanding the relationship between these technologies and BC.

The article served as a foundational piece for this thesis, identifying key areas for further research which the thesis subsequently explored. It stressed the significance of integrating IPA with recognized standards like IEEE 2755.2:2020 and ISO 22301:2019, a theme detailed in the thesis through an analysis of how IPA impacts business continuity. It also highlighted the influence of automation on risk management, explored in depth with a focus on the specific risks associated with RPA in the thesis. Moreover, the article called attention to the need for investigations into governance and human capital dynamics within automation, which the thesis addressed, analysing how these factors are integrated within RPA strategies. Overall, the article laid the groundwork for examining the broader implications of automation technologies in governance, risk management, and compliance, ensuring alignment with business continuity frameworks.

Article details:

- Title: Intelligent Process Automation and Business Continuity: Areas for Future Research.
- Date: 09/02/2023.
- Journal: Information (Switzerland).
- Scimago Journal Rank: Quartile 2 – Information Systems.
- Publisher: MDPI.

information

MDPI

Systematic Review

Intelligent Process Automation and Business Continuity: Areas for Future Research

José Brás [1,2,*], Ruben Pereira [1] and Sérgio Moro [1]

[1] Department of Information Science and Technology, Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR, 999022 Lisboa, Portugal
[2] CGI Innovation Hub Lisbon, 999022 Lisboa, Portugal
* Correspondence: jose_manuel_bras@iscte-iul.pt

Abstract: Robotic process automation and intelligent process automation have gained a foothold in the automation of business processes, using blocks of software (bots). These agents interact with systems through interfaces, replacing human intervention with the aim of improving efficiency, reducing costs and mitigating risks by ensuring and enforcing compliance measures. However, there are aspects of the incorporation of this new reality within the business continuity lifecycle that are still unclear, and which need to be evaluated. This study provides a multivocal literature review of robotic process automation and intelligent process automation correlated with business continuity, to identify the level of awareness of these two emerging forms of automation within the business continuity management lifecycle. Based on the reviewed literature, the study develops a discussion of the main research areas for investigation, identifying what is attracting the attention of practitioners and researchers and which areas they highlight as promising for future research. Numerous sources from relevant backgrounds reveal an interest in these interrelated topics but there as yet is little or no information available on the direct connection between them.

Keywords: business continuity; governance; risk; compliance; robotic process automation; intelligent process automation; business process management

Citation: Brás, J.; Pereira, R.; Moro, S. Intelligent Process Automation and Business Continuity: Areas for Future Research. *Information* **2023**, *14*, 122. https://doi.org/10.3390/info14020122

Academic Editor: Kostas Vergidis

Received: 29 December 2022
Revised: 6 February 2023
Accepted: 9 February 2023
Published: 14 February 2023

1. Introduction

Companies have been on a mission to digitize operations for years, but recent global events, notably the COVID-19 pandemic, have accelerated the process of digital transformation (DT) [1,2] to help organizations grow and cope with instability and disruptions to businesses. Trends such as hyperautomation [3] and hyperconnectivity [4,5] leverage an ever-growing hyperconnected society [6,7] and companies are adopting automated solutions to execute and modernize their business processes (BP) [8] and help ensure business continuity (BC). With automation becoming a new norm for organizations to support their growth and cost optimization strategies, more and more emerging technologies (ET) associated with automation are being adopted, such as robotic process automation (RPA)/intelligent process automation (IPA) [9], intelligent automation (IA) [10], artificial intelligence (AI), and AI-based decision-making tools [11], among others.

RPA/IPA have gained momentum [12], offering solutions to achieve efficiency gains [13] or mitigate organizational problems [14,15]. Figure 1 illustrates the growing interest in the topic, expressed in terms of search results for the keywords from 2010 to 2022 using the Google search engine, thus showing the attention that they have received since 2010.

However, the advent of automation, which potentiates efficiency gains and also resolves problems that result from a lack of human resources, can also create new challenges in terms of dealing with new risks that are still not fully understood [16,17]. Therefore, its impacts on BC must be properly evaluated and require further investigation [15,18,19]. Our research aims to answer the following question: What are the most important areas to investigate in the future with regard to BC and RPA/IPA?

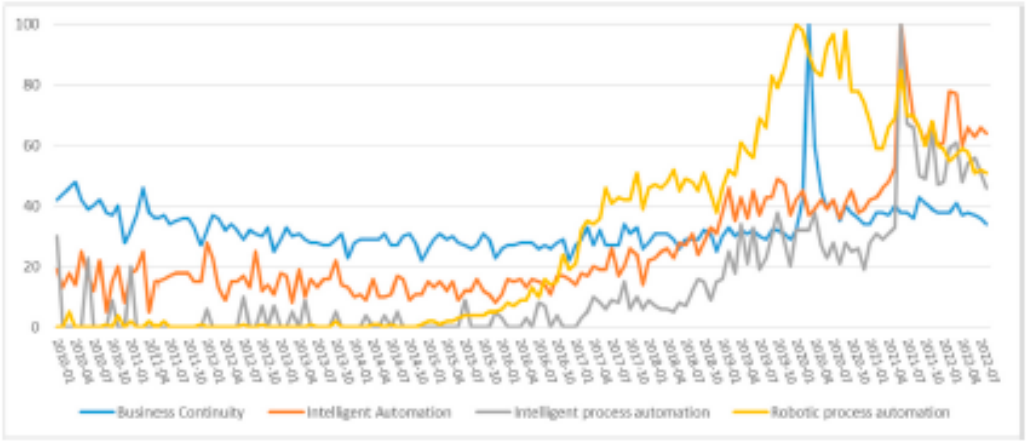


Figure 1. Google trends for BC, RPA, IPA and IA, 2010–2022 (adapted from [20–23]).

The possible need to adopt new procedures for the introduction of new technologies in such a rapid and sometimes disruptive way needs to be properly evaluated in order to adapt and prepare BC for the incorporation of ET such as IPA and RPA. This involves understanding how to promote and develop more flexible recovery strategies appropriate for the new realities, as business processes are now in an almost constant state of change [24,25]. Therefore, it is important to provide companies with insights into how BC professionals can handle business disruptions affecting BP that rely solely on RPA and how to take advantage of this technology to make BC more predictive and less responsive, avoiding disasters by using AI-powered software that can perform these BC-related tasks [26].

This research aims to determine the most important areas to investigate in the future with regard to BC and RPA/IPA. Drawn upon a large body of knowledge, we provide an understanding of the impact on BC resulting from their introduction in organizations, as these two areas together (RPA/IPA and BC) open up a multitude of unknowns that need to be investigated [27–32].

2. Background

2.1. Business Continuity Management

In comparison to the majority of other business management disciplines, business continuity management (BCM) [33,34] is relatively new, as it first appeared in the 1960s as information technology (IT) "disaster recovery" to safeguard company investments in technology; it then gradually evolved, grounded in emerging legislation and standards until 2001 [35]. Figure 2 illustrates the evolution and the major milestones in this process.

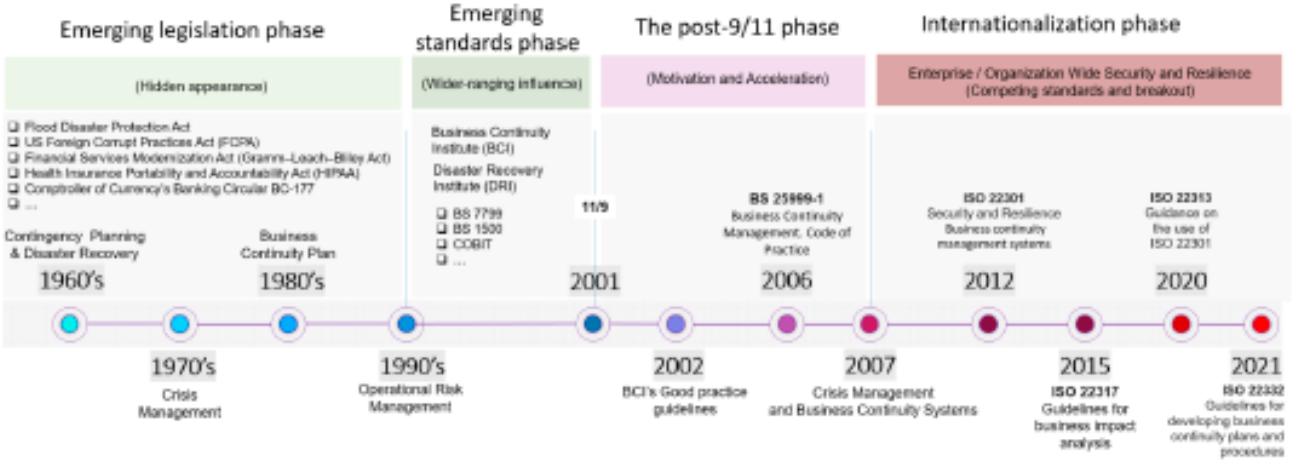


Figure 2. BCM evolution phases (adapted from [27,36]).

Business continuity has become more relevant over time due to disruptive events that have been affecting our lives and businesses: 9/11 in the USA [37], the Islamic state (ISIS) terrorist attacks throughout the world [38], climate changes that affect the planet [39,40], and the recent COVID-19 pandemic [41], which have all shaped the path of BCM (Figure 2). Due to the increasing risk, security, resilience and business continuity [34,42,43] are topics under the radar of corporate consulting services [18,44–48] and industry regulators [33,49]. However, as a result of a larger and constantly hypercompetitive business landscape [2,50], the forces of nature and all other threats present challenges that make it quite difficult for organizations to find objective and consistently effective ways to become resilient and pursue BCM. The level of resilience of an organization or its state of preparedness in terms of facing disasters is crucial to business continuity and IT disaster recovery, as this can mean the difference between success or failure of a company.

A business continuity plan (BCP) and disaster recovery plan (DRP) are not defined in the same way but have similar purposes: both aim to keep an organization operational without disruptions. The BCP is more dedicated to planning the recovery of processes and business functions [19], covering emergency response, business operations continuity, IT disaster recovery and crisis management. The IT DRP is a subset of business continuity, as it is the technical component of the BCP that addresses the recovery of core systems and their data, and enables information and communication technologies (ICT) to continue to operate and support the business.

Business continuity mainly establishes the strategies, procedures and critical actions required to successfully respond to a crisis situation [34]. In addition, it evaluates how well an organization can respond to unexpected disasters, disruptions or sudden changes to its business environment [28,29]. As crises may result from a natural disaster, a catastrophe or just a simple accident that can interrupt services, resulting in the partial or total loss of business [28], a BCP must address all possible situations in order to mitigate or assume undertaken risks.

The British Standards Institution (BCI) defines business continuity as the "capability of the organization to continue the delivery of products or services at acceptable predefined levels following a disruptive event" [29]. It also defines BCM as a "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities" [34]. Furthermore, ISO 22301 [51] specifies that the purpose of a BCP is to provide a documented framework and processes to enable an organization to synthesize all of its business processes within its recovery time objective after a disruptive incident [36].

It is fundamental to define the entire critical process and all the elements needed to perform these tasks in order to ensure business continuity and organizational resilience [30]. One of the main challenges involves proactively elaborating, developing and implementing BCP and DRP and establishing the required knowledge of all the key resources, key activities and key elements [52]. For example, after a disruptive event, an organization needs to establish redesign and re-engineering processes in order to adapt their business to new realities. It is important to note that in a crisis, an organization should have ways, means and tools that enable its operations to continue immediately [34].

To sum up, BCM is an essential tool that aims to ensure that the company is prepared for immediate recovery of its critical activities and their support systems and applications in the event of a disruption.

2.2. Robotic Process Automation and Intelligent Process Automation

These two terms appear to mean the same thing. However, while RPA focuses on automating repetitive tasks and processes based solely on rules, intelligent automation by its very nature incorporates a vast array of ET, such as AI, machine learning (ML),

natural language processing (NLP), structured data interaction, and intelligent document processing [53].

As a relatively recent technology, RPA is preconfigured software that is used to automate a combination of processes, tasks, activities or services, with graphical user interfaces that are choreographed to interact with almost any type of system as a human user would [53,54]. Both scientific research and the media highlight the potential of RPA for increasing the efficiency of processes [55–58]. Since the development of RPA solutions requires low levels of programming experience, with low implementation costs and a very fast return on investments, these solutions are suitable for an extensive wide range of processes and result in very high efficiency gains. Hence, the technology has attracted interest in the business world, with several examples of successful implementation [59].

The initial approach to this technology (intelligent process automation) involved replacing the routine or strictly transactional processes—previously performed by humans and now replaced by RPAs—with solutions capable of performing more complex tasks. As this technology evolved, capabilities related to ML and cognitive computing were added with increasingly sophisticated rule mechanisms, as a result of which it started to be able to perform more complex tasks, including evaluation, reasoning, decision-making and compliance with probabilistic and/or deterministic process requirements in dynamic contexts. Intelligent process automation is thus the evolution of simpler repetitive tasks, in which new capabilities are added with more sophisticated and complex procedures [53,60].

2.3. *Interlinking Intelligent Process Automation with Business Continuity*

In order to fully benefit from automation and address risks, failures or potential threats, organizations need to take a holistic approach to managing change, including alignment between business and IT, BC, and new controls designed to tackle the specific risks emerging from RPA/IPA. Figure 3 summarizes the key activities involving both domains, expressed in actions that illustrate key inter-domain touchpoints for IPA/RPA and BC. It shows the relationship between the two sets of requirements, one for implementation practice and management methodology for intelligent software-based process automation found in IEEE 2755.2-2020, and the other, ISO 22301-2019, pertaining to how the business can implement, maintain and improve a management system to protect from and reduce the likelihood of incidents, and prepare, respond to, and recover from outages when they arise. As this is ongoing research, it is important to find out what should be addressed in order to understand the impacts of the relationship between intelligent process automation and business continuity. Both must be analyzed so that users can develop intelligent software-based process automation or adopt BC procedures that meet the needs of both frameworks.

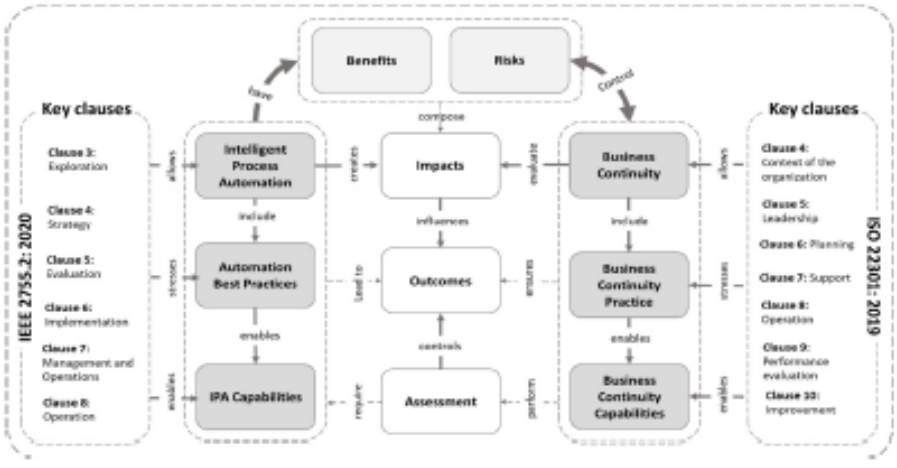


Figure 3. Inter-domain touchpoints for IPA/RPA and BC.

COVID-19 proved that the early adopters who invested in RPA already experienced key returns in 2020, due to the fundamental capabilities that RPA provided for organizations, since RPA can decrease the amount of work for humans, help manage the organization and ensure the continuity of the business [15,61,62]. Although this transformation gained strength through the gains obtained, it created a more complex ecosystem in which a great number of BPs have been updated to incorporate ET associated with RPA, requiring that all risks and benefits need to be re-evaluated to be controlled in terms of BC [63].

Despite academic interest, the topic has received more attention from industry, with several reports being published by various business and senior consulting companies such as Deloitte [61,64], Ernst & Young [65–67], KPMG [68–70] and PwC [63,71,72]. An assessment of the adequacy of BC processes and capabilities/practices to mitigate and support the risks raised by RPA activities is therefore required.

Given the increasing adoption of RPA, the predominant interest of professionals and the lack of systematization and understanding of the main areas of research in RPA and BC, a multivocal literature review (MLR) was conducted to identify the main areas for further investigation.

3. Research Methodology

3.1. Methods

The review protocol specifies the research question being addressed and the methods that are used to perform the review. In order to find the maximum number of studies related to the research question, a search strategy was used to detect as much of the relevant literature as possible using multiple keywords and datasets.

The research was carried out by using search strings to search for information on the main topic, "business continuity", associating it with other interrelated keywords (intelligent automation, intelligent process automation, automation, and RPA). With regard to academic data sources, the publications domain was identified by searching several electronic bibliographic databases, listed below, to build the datasets. The papers were collected on the basis of their title, keywords, abstract, submission for review and publication in academic journals. Google Search (www.google.com (accessed 22 August 2021)) was chosen to search for grey literature.

3.1.1. Data Source and Searches

The PRISMA (preferred reporting items for systematic reviews and meta-analyses) guidelines were followed in the conduct and reporting of this systematic review.

The articles were collected between March and August 2022; and restrictions were applied regarding language (only English) and dates between 2017 and 2022. The following keywords were applied to the search: "business continuity" AND ("robotic process automation" OR "intelligent automation" OR "RPA" OR "IPA" OR "automation" OR "intelligent process automation"). Bibliographies from relevant publications were checked to identify relevant articles.

We searched the following databases for eligible studies:

1. IEEE Xplore Digital Library (https://ieeexplore.ieee.org/Xplore/home.jsp (accessed on 14 June 2021));
2. ACM (https://dl.acm.org (accessed on 1 July 2021)).
3. SpringerLink (https://link.springer.com (accessed on 5 September 2021))
4. Scopus (https://www.scopus.com/home.uri (accessed on 11 November 2021))
5. Web of Science (https://www.webofscience.com/wos/woscc/basic-search (accessed on 2 December 2021))
6. EBSCO (http://search.ebscohost.com/ (accessed on 27 December 2021))
7. Google Search (https://www.google.com/ (accessed on 22 August 2021))

We considered Google Search a limitation in terms of the replicability of the searches performed at a given time but, according to some authors [73], website search methods may differ and it is more important to have a considered rationale for the process, taking

the goals and objectives of each review into account, rather than specifying a single method. The planning and execution of the research, as well as the screening of results and the structure of its management, must be properly organized for this type of approach [73]. They recommend performing a grey literature search using at least one traditional search engine (e.g., Google, Yahoo or Bing) with the first 12 pages (instead of the first 5 pages) and an accurate search of academic databases that are more closely aligned with the topic under analysis, in order to ensure that all the relevant literature is considered and that the conclusions are more comprehensive [74,75].

3.1.2. Eligibility Criteria

For the qualitative analysis, we included articles related to main keywords (process automation or business continuity), present in the title, abstract, key contents or subject relevance. They were found in journals, conference papers, blogs or grey literature (limited to the first 12 pages of Google Search).

3.1.3. Study Selection

In the initial search stage (first filtration, shown in Figure 4), the filtering criteria—inclusion and exclusion criteria filters (all fields; all documents and full text, abstract, reviewed publications in journals, academic journals and grey literature)—were used together with the search string. This step is illustrated in Table 1, as part of the full MLR protocol to find the final sample for the elaboration of the article, which produces a list of the articles found, together with the filters used. All publications that met the inclusion criteria were selected and analyzed.

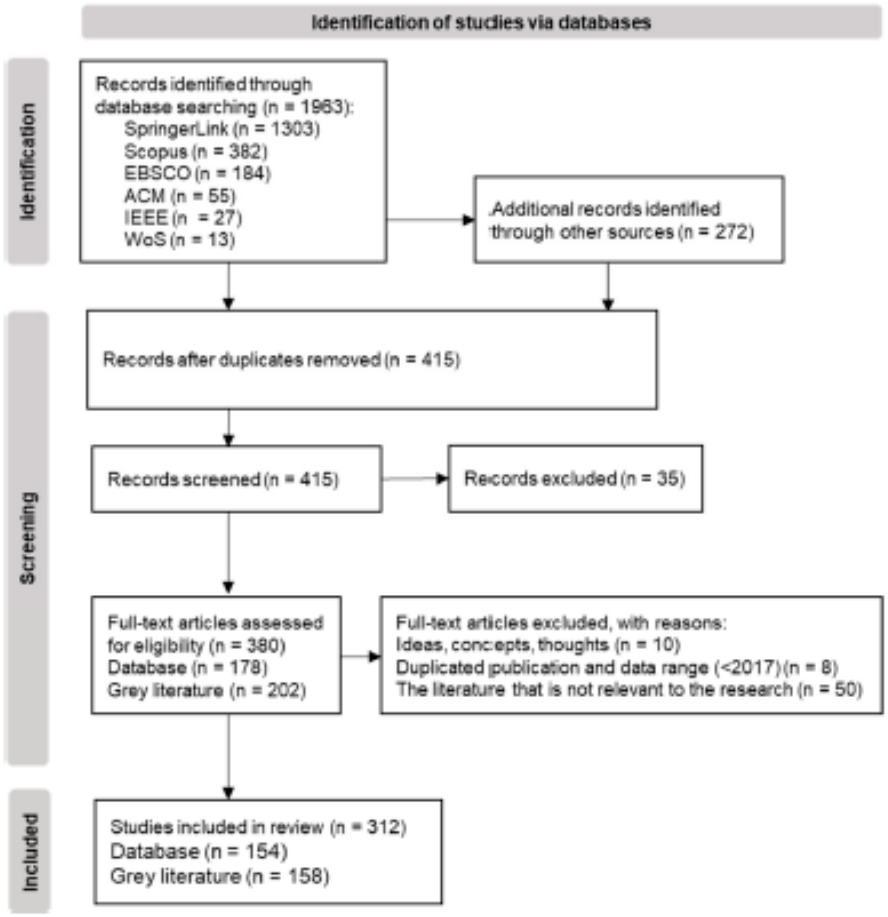


Figure 4. PRISMA Flowchart (adapted from [76]).

Table 2.1 - Inclusion and exclusion criteria used.

Inclusion Criteria	Exclusion Criteria
Related to main keywords	Not related to RPA, IA or IPA or business continuity
Process automation or business continuity	Paper not in English
Title, abstract, key contents or subject relevance	Documents with publication date earlier than 2017
Journals, conference papers, blogs or grey literature	Vendor tool advertisements
Documents in English	Papers by unidentified authors
Limit results to first 12 pages of Google Search	No publication date

In the case of the Google search engine, we consider it to be a valid source of grey literature, governmental and institutional reports. Although Google Search has its limitations and should not be used as the only source for systematic reviews, it was used here as it can be suitable for the purposes of qualitative systematic reviews. For the initial results, only the first twelve pages of the results were counted, which were then used for review and selection [75].

The study has the following research question: What are the most important areas to investigate in the future regarding BC and RPA/IPA?

The overview of the review process can be found in Figure 4, which provides a visual representation of the study selection process that was applied. This diagram represents the different selection steps used in the systematization of the selection process.

An inclusion and exclusion criteria was adopted in order to identify the relevant literature for this study. The screening criteria for including or excluding articles for this research are summarized and illustrated in Table 1.

In order to ensure, whenever possible, the inclusion of all relevant sources, backward and forward snowballing was applied to the set of articles already in the set, as recommended by the systematic review guidelines [77]. Snowballing, in this context, refers to using an article's reference list (backward snowballing) or article citations to identify additional articles (forward snowballing) [77].

A software package (Mendeley) was used to facilitate the task of searching and collecting the literature. This ensures that unique results are obtained, as the software detects and eliminates duplicate entries, thus solving the problem of consistency in the returned and collected results and also organizing it into different sets according to query strings and the academic or grey literature categories. Finally, it facilitates the work of retrieving the results of the distinct ID sets (academic and grey literature) that are easily merged in the study process.

4. Multivocal Literature Review

The multivocal literature review (MLR) [78] is similar to the systematic literature review (SLR) [79,80] and aims to incorporate the so-called "grey literature" in order to supplement the published (formal) literature. MLRs are SLRs which include both scholarly writing (also known as academic writing or formal writing) and the (informal) grey literature (GL) which is not considered in the SLR. GL is considered to be a multisource of information, which may exist in the form of blogs, videos, webpages and white papers that are produced outside academic forums and are not subject to any quality control mechanism (e.g., the peer review process) prior to publication.

By including information that normally would not be taken into account due to its "grey" nature [78], MLRs are important for the completeness of the research. An MLR in a given subject field is essentially a combination of the sources that would be studied in an SLR and a GLR in the same field. Thus, an MLR is, in principle, expected to provide a more complete picture of the evidence in a given field. Figure 5 represents the relationship between SLR, GLR and MLR.

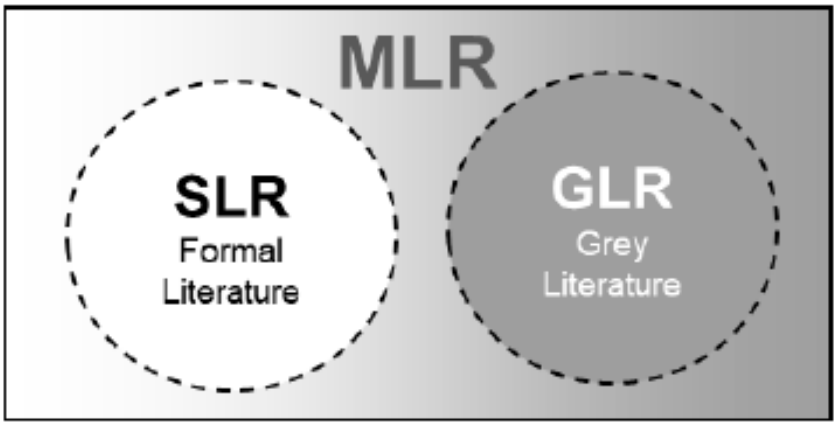


Figure 5. The relationship between SLR, GLR and MLR [78].

The objective is to explore the results of the MLR to provide a state-of-the-art overview of current work on this topic and to identify the most important research areas for BC using IPA, in order to:

1. Identify the most important areas for future research on incorporating RPA/IPA into BC;
2. Outline the definition of objectives for the research;
3. Prepare future surveys and interviews to evaluate the results found, and compare the objectives and the actual observed results from the use of existing projects;
4. Communicate the challenges and opportunities found, the results achieved, and their usefulness for other researchers and professionals (BC practitioners and the RPA/IPA community).

Table 2 distinguishes between "white literature" and "grey literature", listing the appropriate choice of publications in each case. "Black" or other types of literature subject to exclusion are also classified, to clarify the choices made during the assessment.

Table 2. Spectrum of "white", "grey" and excluded literature (adapted from [78]).

"White" Literature	"Grey" Literature	"Black" or Other Types of Literature (Excluded)
Papers published in journals Conference proceedings Books	Preprints e-Prints Lectures Datasets Government documents Standards White papers Technical reports Blogs Audio-video media	Ideas Concepts Thoughts

The MLR workflow is summarized in Figure 6 and has three phases. The initial phase of the research ("planning the MLR") comprises two steps:

- Determining the need for an MLR for the given topic;
- Defining the MLR goal and setting up the research questions.

Once the MLR is planned, we proceed to the next phase of the research, namely "conducting the MLR". This phase is divided into five stages:

- Search process and selection: identification of primary studies to address the research question, application of standard comprehensive search techniques by means of defined search strings, and definition of the selection criteria for performing the selection process;

- Study quality: assessment of sources to determine the extent to which a source is valid and free from bias;
- Design of data extraction: creation of forms to gather all the information needed to address the review question and the study quality criteria;
- Data extraction: extraction of the data items needed to answer the research questions;
- Data synthesis: synthesis of data in such a way that the question(s) can be answered.

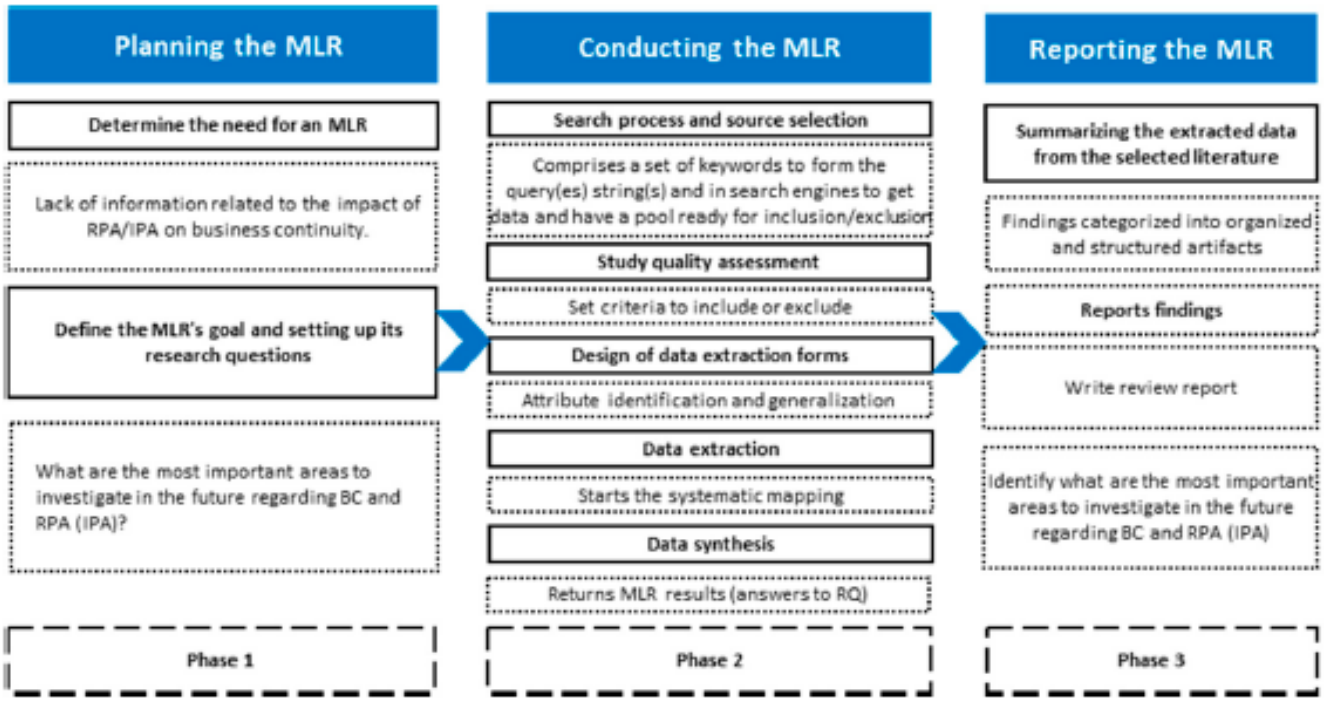


Figure 6. Multivocal literature review (MLR) phases and steps adopted in this research (adapted from [78]).

"Reporting the MLR" is the final phase and is very similar to the SLR guidelines provided by Kitchenham and Charters [81] for planning the MLR, specifying dissemination mechanisms, formatting the main report and evaluating the report.

5. Planning the MLR

Motivation

The COVID-19 pandemic had an impact on organizations, forcing huge changes in several areas which had to be made very quickly. Organizations needed to accelerate the use of digital technology and replace various business processes previously performed in what may be called a "traditional" way with alternative complementary ways of using technology [82]. The most striking examples were related to work roles that were downsized or replaced with technology as a technique to mitigate risks related to infection, while maintaining productivity. Online channels have become the salvation, both for consumers looking for products and also for companies looking for alternative ways to place their products and services on the market. There is a need to implement digital transformation solutions derived from the current state, which is in continuous progress.

However, organizations can also leverage technology to provide business process and service innovations and ensure business continuity [15].

Hence, RPA/IPA have recently become key drivers of digital transformation, supporting process automation more efficiently by replacing repetitive tasks performed by humans and ultimately helping business continuity. Within the domain of business process management, process automation aims to improve the company's workflows, reducing

costs, time and waste, as well as increasing productivity, and reducing errors in processes with technological support, through the application of robotic software to execute tasks.

Another aspect of the motivation for further research in this domain is the fact that RPA/IPA is being widely implemented in many types of organizations, transforming the complexity of the IT environment and business ecosystem even more. The response needed to face new threats and the need to deal with continuous challenges associated with BC is the driving force behind the eventual need to adopt new procedures in order to prepare BC to incorporate RPA and build good flexible recovery strategies [25]. However, management and practitioners need relevant information to support them in incorporating RPA/IPA into BC.

RPA has been attracting a lot of attention from the corporate world. However, although it is a popular topic there, academic research lacks in-depth theoretical analysis of RPA [83]. As a niche area of IT, literature on RPA is rather sparse in terms of its impact on organizations and consequently on business continuity. Further investigation should involve a comprehensive assessment of this technology, identifying guidelines for effective adoption and management and revealing additional factors, as well as the impacts that influence adoption of RPA technology [84].

Since RPA/IPA is being explored more within industry than academia, resulting in important inputs from the former [52,85–87], the MLR expands the origins of the sources to identify and map the most important areas for future investigation related to these two topics.

6. Conducting the MLR

This section describes how the review was conducted, which is the second phase of the process. In this stage, the research is carried out by searching for information in selected databases using the pre-defined queries and analyzing the extracted data.

7. Reporting the MLR

This section presents the organization of the research findings on the most important areas to investigate in the future regarding BC and RPA/IPA.

Our objective is to explore what the (scientific and grey) literature offers in terms of clues to future areas to be investigated. The results were obtained by analyzing and compiling the outcomes found in the results and future work sections of the literature that was analyzed, which led to three meta-themes or clusters: governance, risk management and compliance (GRC); people, processes and technology (PPT); and business continuity (BC). These clusters point to the need for further investigation in order to develop an even more detailed structural research approach to RPA/IPA in combination with business continuity.

Topics related to GRC are summarized in Table 3, in which the "count" column indicates the number of articles found during the investigation that are related to a given topic relevant to each meta theme. Table 4 shows the key findings related to PPT, and Table 5 shows topics related to BC, revealing a direct concern in the literature with how to provide resilient solutions to enable businesses to continue to operate in the event of disruption.

Governance/risk and compliance (Table 3)—commonly known as GRC—is a set of processes and procedures that aim to define a set of rules to assess the activity of organizations (audit procedures, policies and strategic management) to help achieve secure efficiency gains for business objectives, dealing with uncertainty and compliance [16,88,89].

Although it is not a new concept, GRC gained importance as the different types of risks became more numerous, diverse, complex and damaging, thus making it necessary to assess the maturity status of organizations [4,90–93].

The literature that was evaluated also indicated that there is a growing interest in looking for monitoring solutions and a need for new controls to regulate activities in view of the changes imposed by the introduction of RPA and to ensure compliance with the regulatory standards [17,64,94].

Table 4 represents the people/processes/technology grouping (PPT) [95] and its sub-themes which, as autonomous components, are fundamental to organizational transformation and management. In order to achieve organizational efficiency, organizations need to balance these three components and maintain a good relationship between them.

This grouping refers to the methodology in which the balance of people/processes/technology produces outcomes: people perform a specific type of work (using certain capabilities) for an organization using processes (and often technology) to streamline and improve processes [1,3]. This framework helps to achieve balance within an organization and is most often used when deciding whether to purchase or implement new technologies [68]. As these processes now often include different types of technology for diverse solutions, they can represent an increased risk and need to be evaluated according to the appropriate standards and guidelines [42,63,96].

Table 3. Group of key findings related to governance, risk and compliance.

	Key Areas/Subjects for Investigation	Count *
Governance	Types (e-governance/corporate/non-corporate/etc.)	26
	Audit	18
	Policies	13
	Monitoring tools (KPI/Risks)	12
	Strategic management	11
	Productivity	6
	Efficiency gains	4
Risk	Types (avoidance/cyber/digital/financial/environmental/monitoring/organizational/operational/profiling/health and safety/intellectual property protection)	71
	Risk assessment/management	33
	Cybersecurity	29
	Security (assessment/data/mindset/management)	14
	Privacy and security	6
	Enterprise risk management	5
	Security orchestration research and practice	2
Compliance	Monitoring	25
	Regulatory	25
	Controls	17
	Regulatory framework	8

* Number of articles found related to GRC and their subtopics.

Technology is nothing without the right people using the right process to help them and the right guidelines to back them up. Thus, technology should always be the final consideration once a problem is clearly understood, since technology alone does not solve problems. If people do not know how to adapt to change, how to use the technology, which part of the process they are involved in or how to use the process well, technology will not provide the best return on investment and BC may be compromised [97,98].

Table 5 contains subtopics that have a more holistic view of the organization, but are related to BC. According to the British Standards Institution (BSI), "Organizational resilience is the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper" [99]. This helps us to understand that the balance in the people/processes/technology grouping helps create resilience-driven solutions which, in turn, help to enforce GRC in organizations, thus making these topics highly relevant [8,100]. This would, for example, help to avoid disruption in organizations by preparing rapid response/recovery protocols [101]. Understanding which digital or technological threats and impacts are most relevant for better governance of an organization is also on the agenda in the literature [16].

Table 4. Group of key findings related to people/processes/technology.

	Key Areas/Subjects for Investigation	Count *
People	Capabilities to support and ensure BC	69
	Knowledge work/acquisition/management	16
	Human-in-the-loop	10
Processes	Change management	23
	Framework (conceptual/risk/control)	23
	Guidelines	15
	Legislation	8
	Workflows (composition and system)	8
	Standards (create/implement)	7
	Building responding processes and guidelines	7
	Tools/technology/skills	4
	Security orchestration research and practice	2
Technology	Emerging technologies (types/impacts)	53
	Regulatory	8
	Regulatory framework	3

* Number of articles found related to PPT and their subtopics.

Table 5. Key findings for BC.

	Key Areas/Subjects for Investigation	Count *
Business Continuity	Resilience-driven solutions	64
	Governance of new digital/technological threats and impacts	47
	Disruption avoidance	33
	Preparing just-in-case scenarios	8
	Rapid response/recovery protocols	7

* Number of articles related to business continuity and their subtopics.

7.1. Research Areas to Investigate

The authors are aware that this investigation has limitations which future research will need to address. Hence, in line with the research approach, a set of areas to investigate in the future was compiled, resulting from an analysis of the outcomes found in the results and future work sections of the literature. Figure 7 was structured and presented according to three central elements of our research themes (GRC/PPT/BC). These topics are organized in relation to RPA/IPA and BC and have been arranged according to their meta-theme/cluster (GRC/PPT). They emerge from the themes for future investigation indicated in the articles that were analyzed or themes that raised concerns and need more development, compiled from the results found in the articles. In presenting the future areas for investigation, we have added examples from various contexts to make these areas tangible.

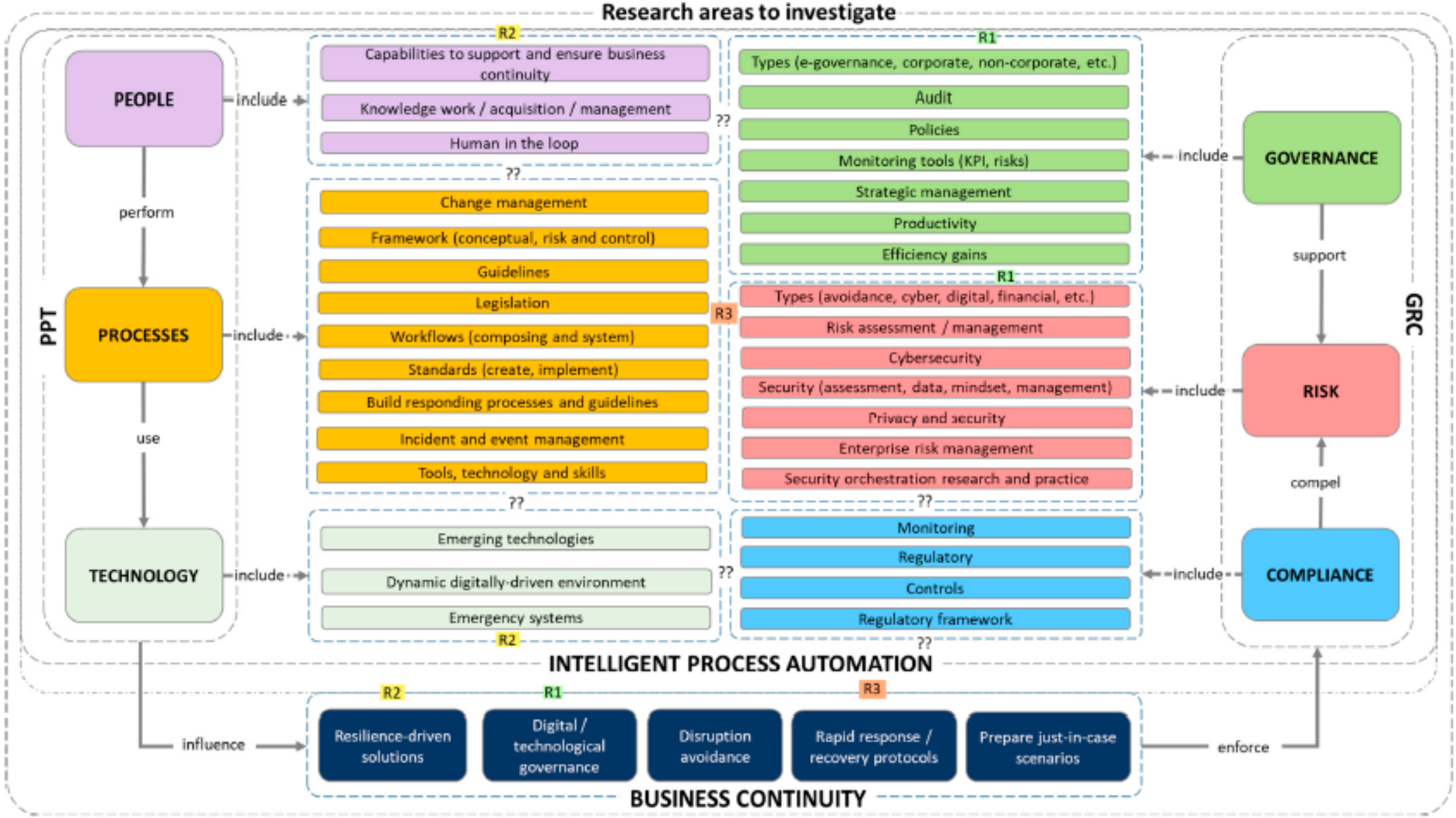


Figure 7. Main areas identified for further investigation.

7.1.1. Governance/Risk/Compliance

In the past, governing boards and directors, as well as senior management, could delegate, ignore or avoid ICT-related decisions. Nowadays, due to the fact that DT and ICT have become crucial to the support, sustainability and growth of enterprises, this topic has become a priority that can no longer be ignored [16,24,102–113].

Types of Governance

A total of 27 papers on this topic show that organizations often underestimate the challenges associated with integrating RPA into their operations, which can leave them vulnerable to risks and facing additional challenges in implementing controls, therefore resulting in governance problems [67,70,101,114]. The solution for mitigating risk in RPA is to follow a strict governance program, and audit rules and controls must therefore be defined correctly [24,92,94,115–124].

Audit Plans

The implementation of process automation programs using RPA/IPA leads to exposure to high risks compared to typical IT automation processes. By analyzing some cases from an audit perspective, we uncovered that there are clear changes in process risk definitions after automation changes in different job functions, impacting access security, considerations related to application change, strategy, and governance of the RPA environment. With more complex environments, auditing/assurance of these ET is becoming more complex than a regular technology audit [26,89,92,118,120,125–135].

Internal Policies

The incorporation of RPA/IPA makes it necessary to adapt or create new internal policies to be integrated into the BC policy [9,50,136–140]. Organizations should document all policies and processes and make this information centrally available so that it can be used for self-learning and training [1,92,132,141].

Types of Risks

A total of 71 results report that some new and disruptive technologies are not well known or understood and can present a range of unknown types of risks if no mitigation response is prepared in advance [142–147]. On the one hand, some literature points to an increased risk arising from the adoption and use of new technologies and the lack of knowledge of their real impact on organizations, while other authors point to evidence that technology helps to mitigate many types of risk [137,148–159]. In addition, organizations need to comply with internal and external regulations and therefore need mechanisms that enable them to respond to legislative concerns about their process activities. This allows them to develop a policy approach focus that reflects technological change, evolving to respond to legislative frameworks and regulatory standards to mitigate risks that arise from the adoption of new technologies or any other situations [110,160,161]. The Digital Operational Resilience Act (DORA) is a concrete realization of these concerns applied to financial institutions [162,163], pinpointing the need to find and implement automated control mechanisms that are fast and flexible to audit, report, share information, and monitor organizations so that their data and information workflows can be understood. It enables their impact on the organization's risk profile to be controlled, by enforcing the implementation of security measures and related testing controls when dealing with information and communication technology (ICT), which also includes RPA/IPA [161,164,165].

Risk Assessment/Management

While RPA can reduce unintended or intentional human errors, adopting RPA/IPA introduces new risks that companies need to understand and address [96,134,166–169]. One of the many risks analyzed comprises those related to cybersecurity, the failure of the organization to consider the effects of operational changes on its internal controls,

or forgetting to update its BC plans [64,65,110]. Failure to properly assess/identify and manage these new risks can erode or limit the entire value created by the adoption of RPA/IPA [170]. In order to grasp the full impacts of automation, companies must consider how RPA affects risk across multiple categories and, at the same time, use its potential to detect those same risks [70,91,171]. For example, AI is attracting great interest as companies explore its ability to unlock value through improved revenues, customer service, efficiency and risk management [112,114,120,132,172].

It is imperative that companies re-evaluate existing BCPs, conduct thorough risk assessments, and identify new vulnerabilities imposed by ET and recent changes in the way we work [29,52,90,94,153,158,172–176].

Monitoring Solutions

An RPA can monitor an extended set of systems in real time according to a wide range of policies and controls [13,140]. BC with continuous monitoring mechanisms is necessary to guarantee the quality associated with the execution of processes, namely for the monitoring of models associated with cognitive components and, at the same time, the integration of AI components in RPA processes, from state control of robots to monitoring changes in their performance [13,48,70,71,94,166,177–179].

As RPA is subject to errors, and resources are needed to ensure detailed monitoring of their operations. This cannot be achieved by using manually monitored controls or a 'wait to see' approach. Monitoring and exception handling mechanisms are needed, and business process management systems (BPMSs) can be used to support these types of issues. In addition to the data collected by RPA/IPA, BPMSs can gather additional information on the execution, duration of execution or properties associated with compliance. This facilitates monitoring by revealing when an RPA process does not behave as expected and by creating alerts leading to immediate maintenance actions on detection of bugs or changes in the requirements of the source applications [87,89,99,124,132,133,179–190].

7.1.2. People/Processes/Technology

Based on the results obtained, there is a perception that organizations are showing a growing interest in seeking out what is new and what is to come in technology [111,177,191,192], although they need to be able to balance these three elements (PPT) to maintain a good relationship between them [97]. This implies preparing the workforce (people) to perform their activities (processes) and choosing the correct tools (technology) to be included [9,24,84,90,104,109,119,120,129,136,141,160,170,178,193–217].

Emerging Technologies

This topic is highlighted in our research in terms of technology, for example in the relevance of AI that is indicated for leveraging IA by combining the strengths of RPA/IPA, AI and human intelligence [63,65,68,105,161,169,218–225]. Now that organizations are beginning to implement technology that has gone beyond the proof-of-concept phases into live systems, the demand for a structured framework to ensure competitiveness, while also guaranteeing the ability to meet the demands of security, regulatory compliance, change management, rapid response to disruptive events and integration with current systems, has become the order of the day [3,10,42,65,90,91,96,129,141,170,178,179,195–200,226–246].

Change Management

References were found signaling the importance for organizations to prepare human workers, not only to provide a solid framework for cooperation with RPA/IPA, but also to mould mentalities and attitudes in relation to change management and new learning [9,119,212,247,248].

In implementing IA, it will be necessary to provide a basis for designing the future workforce that will manage this new reality and also to prepare employees for

the consequences of automation by formulating an appropriate response to managing change [69,201].

An suitable roadmap with all the steps needed to implement the changes required to incorporate new technology will avoid risks associated with IT systems, lack of knowledge, operations and BC (since RPA/IPA do fail and crash) [94,120,126,212,249].

Guidelines

With regard to BC, the Business Continuity Institute (BCI) has compiled a document containing the current national and international legislation, regulations and standards for business continuity management [207]. To ensure resilience, organizations need to have a vision of their capabilities, threats and impacts associated with RPA/IPA and business continuity, and to develop a knowledge structure that will provide guidelines for each business unit that uses automation in the execution of its processes [12,85,140,201,228,250].

Capacity to Support and Ensure BC

Furthermore, 69 of the publications argue that it will be necessary to train teams to support the new processes and activities with new capabilities to support ET and, at the same time, ensure BC [1,3,25,36,45,62,88,92,107,118,136,169,174,184,193,197,198,202–204,211,222,231,233–237,251–293].

The interaction between humans and the automation aspects of BP is also a concern, and guidelines are necessary to regulate these new activities and avoid negative impacts due to neglect or misuse of the technology. Automation projects are not just limited to changing processes and technology, since this necessarily entails fundamental changes in terms of human resources, involving updated skills and responsibilities to respond to new challenges [42,48,97,131,136,148,175,202,231,294–296]. The initial incorporation of these initiatives, together with a properly organized change management program, is of paramount importance to addressing and embracing the human side of the digital modernization initiative. This is critical to avoid disruption and ensure the business continuity [3,47,48,62,69,72,92,97,107,118,131,168,177,277,297–299].

7.1.3. Business Continuity

COVID-19 highlighted the fact that most organizations did not have adequate measures to prepare for BC and disaster recovery [24,34,44,268,300,301], and organizations now realize that they need to find and implement solutions to make them more resilient [172,290,302–305]. RPA platforms, for example, can help and are recommended for making operations more intelligent and for building IT and business resilience [214,215,270,304,306–309].

According to the literature that was reviewed, DT can be an enabler of enterprise resilience since, if it is implemented correctly, it will increase connectivity, transparency, collaboration and innovation [26,261,310–315].

Resilience-Driven Solutions

In order to become resilient, an organization needs to have the ability to anticipate problems and know how to prepare to respond or adapt to sudden changes or interruptions so that it will survive or thrive in the event of disruptive situations [13,25,34,43,47–49,52,82,90,92,94,99,113,213,226,227,229,247,316–321].

Automation adapts to changing market dynamics among organizations, employees and their customers in real time. Operations support processes are also being revamped and will be adapted so that they can respond more quickly to constantly changing environments [88,152,175,182,193,197,222,230,235,253,322–326].

Digital resilience will rely on several areas, including the following:

- The transformation of manual financial services processes (banking/insurance), to respond to changes in market dynamics with greater flexibility, effective communication and confidence;

- Optimizing resource management using automation and predictive analytics to determine where technicians and maintenance personnel should be deployed;
- Enabling rapid business DT with adaptable and resilient business models to enhance relationships with customers, and ensure they benefit from greater value in the process outsourcing services provided, through deeper collaboration and co-innovation [51,85,100,194,262,268,269,279,280,295,306,307,310,314,326–336].

Governance of New Digital/Technological Threats and Their Impacts

A DT project involves multiple factors in the transformation of the business model, impacting the entire organization—especially operational processes, resources and internal and external users—since it involves a major change in habits and ways of working, based on collaboration and intensive interactions [140,213,259,260,313,326,331,337–346].

These changes present different types of impacts as well as threats, such as those linked to the incorporation of ET smart products and services, as well as the ways in which organizations interact with their customers, improve operational efficiency, increase revenue, strengthen the competitiveness of offerings and improve customer experience. In order for organizations to have a clear vision of what to expect regarding these changes, it will be necessary to reassess the risks and their governance practices [93,96,142,153,156,180,198,232,254,304,347–349].

A properly structured program is required for identification and protection against digital risks, as part of a unified DT plan that includes several elements, such as the selection of appropriate digital technology and its implementation, and protection measures against digital threats from new technologies: moreover, it must clearly understand their (positive/negative) impacts [4,9,14–16,46,47,52,53,90,91,99,121,129,136,177,350,351].

Disruption Avoidance

Avoiding disruption to a particular business service support system or process can be seen as a contributing factor to operational resilience. However, the phenomena that lead to disruptions are very complex and non-linear and no satisfactory model has yet been developed to avoid them or predict when they will occur and what kind of impacts they will cause. For this reason, the ML and AI techniques associated with RPA/IPA have begun to be widely used in recent years [8,10,26,85,104,115,131,145,148,152,176,201,204,215,217,260,272,278,290,295,299,304,311,312,314,325,329–331,352–357].

7.2. Findings

Figure 7 illustrates the proposed framework and is composed of three meta-themes or clusters: governance, risk management, and compliance (GRC); people, processes and technology (PPT); and business continuity (BC). These clusters suggest further investigation in order to develop an even more detailed structural research approach to RPA/IPA in combination with business continuity. The framework was developed to incorporate future research areas. It should be noted that the inter-domain touchpoints, shown as "??", represent the existing uncertainties to explore, and R1, R2 and R3 are relations that have already been discussed in the literature but need to be evaluated and further investigated.

All the topics that are synthesized in Figure 7 are findings that were organized according to the topics of governance, risk, and compliance (GRC), and to people, processes, and technology (PPT). All of them are associated with both robotic process automation and business continuity, showing the direct interest evidenced in the literature with how to provide resilient solutions to allow businesses to continue to operate in case of disruption.

The PPT cluster in Figure 7 shows the group of people that performs processes that include technology, emphasizing that organizations need to incorporate in-the-loop knowledge workers with the right capabilities/functionalities to support and ensure BC. Moreover, these workers will need to use processes based on updated guidelines, legislation, standards and applicable frameworks. The technology enables ET such as RPA/IPA, AI or blockchain and will balance the two other elements (people and processes) by lever-

aging their capabilities while, at the same time, creating solutions for BC that allow for organizational resilience.

Another priority emerges from the literature on the enforcement of GRC in relation to BC topics, which points to preparing organizations to be more resilient and responsive. Although there are only a few specific topics regarding BC, all the reviewed literature refers to the association between RPA/IPA/Automation and BC; in this way therefore, all the constituents of the macro topics contribute in the same way to BC.

The analysis of the GRC cluster revealed quite a few references to topics of interest, such as the regulatory framework, control, regulatory and monitoring solutions that define organizational compliance when applying policies, relevant laws, and regulations. Risk is the macro topic that is attracting most interest in the literature found, and hence it is necessary to assess which types of risk are raising the most concerns—privacy, security avoidance, cyber or financial—in order to detect which threats could have a negative impact on an organization's ability to conduct business.

Finally, the results for governance in terms of number of publications indicate that in order to steer an organization towards BC, topics such as auditing, policies, monitoring tools (applied to GRC), strategic management, productivity and efficiency gains, are on the agenda.

Although it was not the main goal of this research, some evidence of relationships could be found in the literature. They include governance/cyber risks and business continuity, expressed as R1 [93], which highlights the need for qualifications for all levels of the business in emerging areas of risk in the preparation of business continuity plans, and governance for cyber-attacks, both in the short and long term as a preventive measure. Another relation found, R2, concerns the role of emerging and intelligent technologies in the design and development of responsive supply chains, enhancing their capacity to ensure business continuity [197]. R3 is related to the publication of a legislative proposal to create a digital operational resilience framework for the EU financial services sector. It relates legislation, guidelines, and incident and event management from the PPT cluster, on the one hand, to the GRC cluster for risk assessment, cyber and digital risk themes present in the business continuity cluster [162], on the other.

8. Conclusions

This study presents an MLR on RPA/IPA correlated with BC, aiming to identify the state of awareness of RPA/IPA within the BCM lifecycle and to highlight areas for future research. In the course of our research, we realized that digital solutions providers have started to publicize and present RPA and IA as a business continuity enabler [220,320,321,358–360].

For professionals, this survey identifies themes that should be on the agenda for BC and DT using ET. RPA/IPA can be very useful and can leverage daily operations but may contain risks that need to be properly understood, monitored, controlled and addressed. Hence, organizations should update their policies and guidelines to ensure they reflect audit capabilities that allow for secure monitoring of all the changes that are being incorporated into their businesses. Another important aspect concerns the need to provide the necessary tools, knowledge and skills to their members, so that they are able to face new challenges that may arise due to the incorporation of certain kinds of ET.

In providing an initial conceptualization of the interplay between RPA/IPA and business continuity, as well as presenting and discussing related areas for future research, we hope our results stimulate broad discussion within the community on the possible adaptations of processes that have received little attention to date, but which we consider highly relevant.

The highlighted results are not based on the total number of articles found per cluster, as many of the articles are associated with a variety of themes, but on the theme that stands out most in each case.

In the case of the GRC cluster, the subtopic with the most results was the risk topic—"Types of risks" to be analyzed, associated with IPA/RPA and business continuity. In the PPT cluster, it was the capabilities associated with people and RPA/IPA required to

support BC that was most underlined. Finally, in the BC cluster, a large number of articles highlighted the need to find resilience-oriented solutions. These themes will be prioritized in our future research.

Figure 7 summarizes the findings and can guide academics towards topics that merit further investigation, namely:

- Which threats and impacts organizations may expect when incorporating RPA/IPA into businesses;
- Mapping risks emerging from the use of RPA/IPA and finding ways to mitigate them;
- Resilience-driven solutions for dealing with known threats and impacts, in particular those emerging from the use of RPA/IPA;
- The new capabilities associated with RPA/IPA that are more useful in terms of supporting and ensuring BC;
- Ways to incorporate governance measures to deal with new RPA/IPA threats and impacts and avoid disruption;
- Correlation of all the identified topics with BC and RPA or IPA, in order to find solutions that can mitigate possible risks, while at the same time taking advantage of their benefits;
- ICT support for all the innovative and complex systems used in this new digital age. Greater digitization, automation, interconnectivity, and also their interdependency, amplify ICT risks, making society as a whole—and the financial system in particular—more vulnerable to cyber threats or ICT disruptions. Although the universal use of ICT systems and the high level of digitization, automation and connectivity (where RPA/IPA is included) are currently essential features of all global activities, digital resilience is still not sufficiently integrated into the operational frameworks of organizations, and there is therefore a need for research into how to evolve in this area [106,162].

As with many other studies, ours has limitations which future research needs to address. Most significantly, the areas presented for future investigation were derived from the individual contributions of researchers working in RPA/IPA and BC and from grey literature. While we cannot formally claim the integrity and validity of our results, our approach is in line with common standards and guidelines for conducting qualitative research. Nevertheless, future research should explore these areas of investigation more rigorously (e.g., as the subject of Masters' theses, using exploratory interviews, focus groups, or the Delphi method).

Author Contributions: Conceptualization, J.B. and R.P.; methodology, J.B.; validation, R.P. and S.M.; formal analysis, J.B.; investigation, J.B.; resources J.B.; writing—original draft preparation, J.B.; writing—review and editing, J.B. and Ruben; visualization J.B.; supervision, R.P. and S.M.; project administration, R.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data was created.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shivakumar, S.K.; Sethii, S. *Building Digital Experience Platforms*; Springer: Berlin/Heidelberg, Germany, 2019. [CrossRef]
2. Henderson, A.D.; Graebner, M.E. Entering a Golden Age of Sustained Superiority: Entrepreneurial Creation or Discovery? *Organ. Sci.* **2020**, *31*, 1432–1451. [CrossRef]
3. Lasso-Rodriguez, G.; Winkler, K. Hyperautomation to fulfil jobs rather than executing tasks: The BPM manager robot vs human case. *Rom. J. Inf. Technol. Autom. Control* **2020**, *30*, 7–22. [CrossRef]
4. Gaines, B.R. From facilitating interactivity to managing hyperconnectivity: 50 years of human–computer studies. *Int. J. Human-Computer Stud.* **2019**, *131*, 4–22. [CrossRef]
5. Moreolo, M.S.; Fabrega, J.M.; Nadal, L.; Martinez, R.; Casellas, R. Synergy of Photonic Technologies and Software-Defined Networking in the Hyperconnectivity Era. *J. Light. Technol.* **2019**, *37*, 3902–3910. [CrossRef]

6. Bradai, A.; Rehmani, M.H.; Haque, I.; Nogueira, M.; Bukhari, S.H.R. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for a Hyperconnected World: Challenges, Applications, and Major Advancements. *J. Netw. Syst. Manag.* **2020**, *28*, 433–435. [CrossRef]
7. González-Larrea, B.; Hernández-Serrano, M.J. Digital identity built through social networks. In Proceedings of the Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality, Salamanca, Spain, 21–23 October 2020. [CrossRef]
8. Taulli, T. *The Robotic Process Automation Handbook*; Springer: Berlin/Heidelberg, Germany, 2020. [CrossRef]
9. Lacity, M.; Willcocks, L.P. *Dynamic Innovation in Outsourcing*; Springer: Berlin/Heidelberg, Germany, 2018. [CrossRef]
10. Datamatics Digital Adoption–Intelligent Automation Powered Chatbots to Ensure Business Continuity in Services Industry. 2021. Available online: https://www.datamatics.com/hubfs/DatamaticsWebsiteWhitepapers/2021WhitepaperPDFs/Digital-Adoption--Intelligent-Automation-Powered-Chatbots-To-Ensure-Business-Continuity-In-Services-Industry.pdf (accessed on 22 June 2021).
11. Nicodeme, C. Build confidence and acceptance of AI-based decision support systems—Explainable and liable AI. In Proceedings of the 2020 13th International Conference on Human System Interaction (HSI), Tokyo, Japan, 6–8 June 2020; pp. 20–23. [CrossRef]
12. Deloitte Robotic and Cognitive Automation. 2017. Available online: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-seminar-2017-robotic-cognitive-automation.pdf (accessed on 22 June 2021).
13. Kapoor, S.; Sagar, A. New Principles of Business Continuity and Acceleration, Made Possible with Automation. No. July. 2020. pp. 1–12. Available online: https://www.cdotrends.com/white-paper/15621/new-principles-business-continuity-and-acceleration (accessed on 25 July 2021).
14. Yang, J.; Kumar, V.; Ekren, B.; Kuzmin, E. Understanding the Role of Digital Technologies in Supply Chain Risks Management. *Digit. Transform. Ind. Trends Manag. Strateg.* **2021**, *44*, 133–146. [CrossRef]
15. Siderska, J. The Adoption of Robotic Process Automation Technology to Ensure Business Processes during the COVID-19 Pandemic. *Sustainability* **2021**, *13*, 8020. [CrossRef]
16. von Solms, J.; Langerman, J. *Risks and Threats Arising from the Adoption of Digital Technology in Treasury*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 1339.
17. Green, J.S.; Daniels, S. Information and cyber security. In *Digital Governance*; Routledge: Abingdon-on-Thames, UK, 2019; pp. 173–199. [CrossRef]
18. Capgemini Business Continuity Planning. 2016. Available online: https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/business-continuity-planning.pdf (accessed on 13 March 2021).
19. Tashi, S.G.-H.I.; Tashi, I.; Ghernaouti-Hélie, S. Information Security Evaluation: A Holistic Approach from a Business Perspective-Igli Tashi, Solange Ghernaouti-Helie. Presses Polytechniques Et Universitaires Romandes. 1 January 2011. Available online: https://books.google.pt/books?id=UBHIAgAAQBAJ (accessed on 13 March 2021).
20. Google Intelligent Process Automation-Google Trends. 2022. Available online: https://trends.google.com/trends/explore?date=2010-01-012022-08-31&q=Intelligentprocessautomation#TIMESERIES (accessed on 1 September 2022).
21. Google Robotic Process Automation-Google Trends. 2022. Available online: https://trends.google.com/trends/explore?date=2010-01-012022-08-31&q=Roboticprocessautomation#TIMESERIES (accessed on 1 September 2022).
22. Google Intelligent Automation-Google Trends. 2022. Available online: https://trends.google.com/trends/explore?date=2010-01-012022-08-31&q=IntelligentAutomation#TIMESERIES (accessed on 1 September 2022).
23. Google Business Continuity-Google Trends. 2022. Available online: https://trends.google.com/trends/explore?date=2010-01-012022-08-31&q=BusinessContinuity#TIMESERIES (accessed on 1 September 2022).
24. Röglinger, M.; Plattfaut, R.; Borghoff, V.; Kerpedzhiev, G.; Becker, J.; Beverungen, D.; Brocke, J.V.; Van Looy, A.; Del-Rio-Ortega, A.; Rinderle-Ma, S.; et al. Exogenous Shocks and Business Process Management. *Bus. Inf. Syst. Eng.* **2022**, *64*, 669–687. [CrossRef]
25. Elgazzar, Y.; El-Shahawy, R.; Senousy, Y. *The Role of Digital Transformation in Enhancing Business Resilience with Pandemic of COVID-19*; Lecture Notes in Networks and Systems; Springer: Berlin/Heidelberg, Germany, 2021; pp. 323–333. [CrossRef]
26. Deloitte Auditing the RPA Environment Our Approach towards Addressing Risks in a BOT Environment Risk Advisory. 2018. Available online: www.deloitte.com/about (accessed on 22 August 2021).
27. Herbane, B. The evolution of business continuity management: A historical review of practices and drivers. *Bus. Hist.* **2010**, *52*, 978–1002. [CrossRef]
28. Zhang, H.; Bie, Z.; Li, G.; Lin, Y. Assessment method and metrics of power system resilience after disasters. *J. Eng.* **2019**, *2019*, 880–883. [CrossRef]
29. BCI Business Continuity, Preparing for Challenges under a 'New Normal' Paradigm. 2021. Available online: https://www.thebci.org/news/business-continuity-preparing-for-challenges-under-a-new-normal-paradigm.html (accessed on 30 October 2021).
30. Hiles, A. The Definitive Handbook of Business Continuity Management. 2010. Available online: https://books.google.pt/books?id=iDyoSoeoIDusC&printsec=frontcover&dq=The+definitive+handbook+of+business+continuity+management&hl=pt-PT&sa=X&ved=2ahUKEwiSuojqLDvAhWWDGMBHbgMCoYQ6AEwAHoECAMQAg#v=onepage&q= (accessed on 22 August 2021).
31. Kliem, R.L. *Business Continuity Planning. Business Continuity Planning: A Project Management Approach*; CRC Press: Boca Raton, FL, USA, 2015. [CrossRef]
32. Hamid, A. Limitations and challenges towards an effective business continuity management in Nuklear Malaysia. *IOP Conf. Series: Mater. Sci. Eng.* **2018**, *298*, 012050. [CrossRef]

33. Business Continuity Institute. *BCM Legislations, Regulations, Standards and Good Practice*; no. February; Business Continuity Institute: Reading, UK, 2020; pp. 1–114.
34. *ISO 22301*; 2019 Security and Resilience—Business Continuity Management Systems—Requirements. ISO: Geneva, Switzerland, 2019.
35. Hiles, A. Business Continuity Management: Global Best Practices. 2014. Available online: https://books.google.pt/books?id=VyxpCgAAQBAJ&printsec=frontcover&dq=Business+Continuity+management&hl=pt-PT&sa=X&redir_esc=y#v=onepage&q=BusinessContinuitymanagement&f=false (accessed on 21 August 2021).
36. Brás, J.C.; Ribeiro, R. Business Continuity and Disaster Recovery: New Trends and Challenges. In Proceedings of the 13ª CONTECSI -International Conference on Information Systems and Technology Management, Regensburg, Germany, 1–3 June 2016. [CrossRef]
37. Barbara, M. *Determining the Critical Success factors of an Effective Business Continuity/Disaster Recovery Program in a Post 9/11 World: A Multi-Method Approach*; Concordia University: Montréal, QC, Canada, 2006.
38. Michel-Kerjan, E.; Pedell, B. Terrorism Risk Coverage in the Post-9/11 Era: A Comparison of New Public–Private Partnerships in France, Germany and the U.S. *Geneva Pap. Risk Insur.* **2005**, *30*, 144–170. [CrossRef]
39. Forino, G.; von Meding, J. Climate change adaptation across businesses in Australia: Interpretations, implementations, and interactions. *Environ. Dev. Sustain.* **2021**, *23*, 18540–18555. [CrossRef]
40. Kaur, A.; Kumar, A.; Luthra, S. Business continuity through customer engagement in sustainable supply chain management: Outlining the enablers to manage disruption. *Environ. Sci. Pollut. Res.* **2021**, *29*, 14999–15017. [CrossRef]
41. Kapoor, K.; Bigdeli, A.Z.; Dwivedi, Y.K.; Raman, R. How is COVID-19 altering the manufacturing landscape? A literature review of imminent challenges and management interventions. *Ann. Oper. Res.* **2021**, 1–33. [CrossRef] [PubMed]
42. Moore, P.V. OSH and the Future of Work: Benefits and Risks of Artificial Intelligence Tools in Workplaces. In *Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management. Human Body and Motion*; Springer: Cham, Switzerland, 2019; Volume 11581. [CrossRef]
43. ISO/IEC 25010:2011 Systems and Software Engineering—Systems and Software Quality Requirements and Evaluation (SQuaRE)—System and Software Quality Models. 2011. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en (accessed on 24 August 2021).
44. CGI Disaster Recovery as a Service. Promedia Technology Solutions. 2015. Available online: https://www.promedianj.com/infrastructure/cloud-services-private-public-hybrid/disaster-recovery-as-a-service (accessed on 22 August 2021).
45. IBM Maintain Business Continuity. 2020. Available online: https://www.ibm.com/services/business-continuity (accessed on 13 March 2021).
46. KPMG Business Continuity in a COVID-19 World. 14 August 2020. Available online: https://home.kpmg/xx/en/home/insights/2020/03/business-continuity-in-a-covid-19-world.html (accessed on 10 January 2021).
47. BCG The Digital Path to Business Resilience | BCG. 2020. Available online: https://www.bcg.com/publications/2020/digital-path-to-business-resilience (accessed on 13 March 2021).
48. Accenture COVID-19: Business Continuity Planning. 2020. Available online: https://www.accenture.com/cz-en/insights/operations/coronavirus-effective-business-operations (accessed on 13 March 2021).
49. BCI Leveraging BCM Automation to Enhance Organizational Resilience. 2019. Available online: https://www.thebci.org/news/leveraging-bcm-automation-to-enhance-organizational-resilience.html (accessed on 7 November 2021).
50. D'Aveni, R.A. Waking up to the new era of hypercompetition. *Wash. Q.* **1998**, *21*, 183–195. [CrossRef]
51. BSI ISO 22301-Self-Assessment Questionnaire-How Ready Are You? 2016. Available online: https://www.bsigroup.com/Documents/iso-22301/resources/iso-22301-self-assessment-form-2016.pdf (accessed on 3 March 2021).
52. Păunescu, C.; Argatu, R. Critical Functions in Ensuring Effective Business Continuity Management. Evidence from Romanian Companies. *J. Bus. Econ. Manag.* **2020**, *21*, 497–520. [CrossRef]
53. *2755-2017-EEE Guide for Terms and Concepts in Intelligent Process Automation*; IEEE: Piscataway, NJ, USA, 2017; pp. 1–16. [CrossRef]
54. Kregel, I.; Koch, J.; Plattfaut, R. Beyond the Hype: Robotic Process Automation's Public Perception over Time. *J. Organ. Comput. Electron. Commer.* **2021**, *31*, 130–150. [CrossRef]
55. Herm, L.-V.; Janiesch, C.; Helm, A.; Imgrund, F.; Hofmann, A.; Winkelmann, A. A framework for implementing robotic process automation projects. *Inf. Syst. E-Business Manag.* **2022**, 1–35. [CrossRef]
56. Villar, A.S.; Khan, N. Robotic process automation in banking industry: A case study on Deutsche Bank. *J. Bank. Financial Technol.* **2021**, *5*, 71–86. [CrossRef]
57. Behrens, K. Benefit of RPA: Efficiency. 2015. Available online: https://www.uipath.com/blog/rpa/benefit-of-rpa-efficiency (accessed on 30 January 2023).
58. O'Donnell, J. RPA in Manufacturing Increases Efficiency, Reduces Costs | TechTarget. 2019. Available online: https://www.techtarget.com/searcherp/feature/RPA-in-manufacturing-increases-efficiency-reduces-costs (accessed on 30 January 2023).
59. SA, I. Bringing Clarity and Objective Guidance to Software Based Intelligent Process Automation Space. Available online: https://beyondstandards.ieee.org/ieee-2755-standards-to-bring-clarity-and-objective-guidance-to-software-based-intelligent-process-automation-space/ (accessed on 22 March 2021).

60. IEEE P2755.2/D. IEEE Approved Draft Recommended Practice for Implementation and Management Methodology for Software Based Intelligent Process Automation (SBIPA). IEEE P2755.2/D2, September 2020. pp. 1–58. Available online: https://ieeexplore.ieee.org/document/9199584 (accessed on 17 March 2021).
61. Deloitte Internal Controls over Financial Reporting Considerations for Developing and Implementing Bots. No. September. 2018. pp. 1–8. Available online: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-internal-controls-over-financial-reporting-considerations-for-developing-and-implementing-bots.pdf (accessed on 24 August 2021).
62. DXC How Integrated Intelligent Automation Can Modernize Legacy ERP. 2021. Available online: https://dxc.com/us/en/insights/perspectives/paper/how-integrated-intelligent-automation-can-modernize-legacy-erp (accessed on 1 November 2021).
63. PwC Emerging & Disruptive Technology Risk: Stayin in Control of Your Emerging Technologies. 2018. Available online: https://www.pwc.co.uk/services/risk/technology/emerging-disruptive-technology-risk-stay-in-control.html (accessed on 24 October 2021).
64. Deloitte How Does RPA Affect You? 2018. Available online: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-icfr-refocus-your-robotic-process-automation-lens.pdf (accessed on 24 August 2021).
65. Intelligent Automation in Financial Services. 2021. Available online: https://www.ey.com/engl/intelligent-automation-in-financial-services (accessed on 24 October 2021).
66. Five Design Principles to Help Build Confidence in RPA Implementations. 2019. Available online: https://www.ey.com/engl/consulting/five-design-principles-to-help-build-confidence-in-rpa-implement (accessed on 24 October 2021).
67. Insights for Executives. No. February. 2017. pp. 1–8. Available online: https://assets.ey.com/content/dam/ey-sites/ey-com/engl/topics/advisory/ey-robotics-process-automation-5-Series.pdf?download (accessed on 24 August 2021).
68. Cline, B.; Henry, M.; Justice, C. Rise of the robots. *Aviat. Week Space Technol.* **2016**, *178*, 56–61.
69. KPMG Manage the Effects of Robotic Process Automation. 2019. Available online: https://assets.kpmg/content/dam/kpmg/nl/pdf/2019/advisory/manage-the-effects-of-rpa-to-enable-a-future-proof-workforce.pdf (accessed on 24 October 2021).
70. KPMG Automation: The Upside of the Pandemic and the Future. 2021. Available online: https://home.kpmg/uk/en/blogs/home/posts/2021/09/automation-the-upside-of-the-pandemic-and-the-future-of-controls.html (accessed on 24 October 2021).
71. PwC Robotic Process Automation-Friend or Foe for Your Risk Profile? no. March. 2016. Available online: https://www.pwc.com.au/pdf/pwc-article-rpa-friend-or-foe-for-your-risk-profile.pdf (accessed on 21 August 2021).
72. PwC Globa Crisis Survey 2021. Pwc, No. March. 2021. Available online: https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html (accessed on 24 August 2021).
73. Stansfield, C.; Dickson, K.; Bangpan, M. Exploring issues in the conduct of website searching and other online sources for systematic reviews: How can we be systematic? *Syst. Rev.* **2016**, *5*, 1–9. [CrossRef]
74. Bellefontaine, S.P.; Lee, C.M. Between Black and White: Examining Grey Literature in Meta-analyses of Psychological Research. *J. Child Fam. Stud.* **2013**, *23*, 1378–1388. [CrossRef]
75. Coleman, S.; Wright, J.M.; Nixon, J.; Schoonhoven, L.; Twiddy, M.; Greenhalgh, J. Searching for Programme theories for a realist evaluation: A case study comparing an academic database search and a simple Google search. *BMC Med. Res. Methodol.* **2020**, *20*, 1–10. [CrossRef]
76. Jones, M.A.E. LibGuides: Systematic Reviews: Step 8: Write the Review. Available online: https://guides.lib.unc.edu/systematic-reviews/write (accessed on 5 February 2023).
77. Wohlin, C. Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, London, UK, 13–14 May 2014; pp. 1–10.
78. Garousi, V.; Felderer, M.; Mäntylä, M.V. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inf. Softw. Technol.* **2019**, *106*, 101–121. [CrossRef]
79. Garousi, V.; Felderer, M.; Mäntylä, M.V. The need for multivocal literature reviews in software engineering. *ACM Int. Conf. Proceeding Ser.* **2016**, *26*, 6. [CrossRef]
80. Kitchenham, B. Guidelines for Performing Systematic Literature Reviews in Software Engineering. 2007. Available online: https://www.elsevier.com/data/promismisc/525444systematicreviewsguide.pdf (accessed on 3 April 2022).
81. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical report, Ver.2.3 EBSE; EBSE: Delhi, India, 2007; 20p, Available online: https://www.cs.auckland.ac.nz/~{}norsaremah/2007%20Guidelines%20for%20performing%20SLR%20in%20SE%20v2.3.pdf (accessed on 24 August 2021).
82. Swain, A.K.; Garza, V.R. Key Factors in Achieving Service Level Agreements (SLA) for Information Technology (IT) Incident Resolution. *Inf. Syst. Front.* **2022**, *1*, 1–16. [CrossRef]
83. Chugh, R.; Macht, S.; Hossain, R. Robotic Process Automation: A review of organizational grey literature. *Int. J. Inf. Syst. Proj. Manag.* **2022**, *10*, 5–26. [CrossRef]
84. Aldossari, M.; Zin, A.M. The use of automation and robotic innovations in the transformational companies: Systematic literature review. *J. Theor. Appl. Inf. Technol.* **2019**, *97*, 3661–3690.
85. Theuerkauf, J. Rethinking Business Continuity Plans, Phase One: Initializing RPA Deployment. 19 June 2021. Available online: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/06/19/rethinking-business-continuity-plans-phase-one-initializing-rpa-deployment/?sh=42b038514bdc (accessed on 25 July 2021).

86. PwC Three Key Considerations for AI and RPA Risk Management. 2021. Available online: https://proedge.pwc.com/ai-and-rpa-risk-management (accessed on 24 August 2021).
87. Salierno, D. Tech Adoption Falls Short. Internal Auditor, vol. 75, iss. 5, pp. 11–12, October, 2018. Available online: https://iia-indonesia.org/files/magazine/Majalah_IA_Oct2018.pdf (accessed on 24 August 2021).
88. Carias, J.F.; Borges, M.R.S.; Labaka, L.; Arrizabalaga, S.; Hernantes, J. Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access* **2020**, *8*, 174200–174221. [CrossRef]
89. Deloitte Risk Management throughout the Robotics Process. No. December. 2020. Available online: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/DeloitteBelgiumRPABrochure.pdf (accessed on 24 August 2021).
90. Alvero, K.M.; Cassels, W. Bringing Clarity to the Foggy World of AI. Internal Auditor, no. February, 2020. pp. 46–50. Available online: https://internalauditor.theiia.org/en/articles/2020/february/bringing-clarity-to-the-foggy-world-of-ai/ (accessed on 24 August 2021).
91. Chigurupati, M. Intelligent Automation to Renew Business Continuity Priorities. 2020. Available online: https://www.lntinfotech.com/blogs/intelligent-automation-the-herculean-tool-to-renew-business-continuity-priorities-during-a-pandemic/ (accessed on 1 August 2021).
92. Lee, Y.; Li, W.-S.; Liu, Y.-C.; Chen, K.-H.; Chang, C.-L.; Watanabe, K. Applying Information Technology for Cross Border Disaster Risk Reduction Through Public Private Partnership Amidst COVID-19. *IFIP Adv. Inf. Commun. Technol* **2021**, *622*, 57–72. [CrossRef]
93. Guerin, T. Questions that board directors should be asking about emerging governance issues and risk: A practitioner's view and implications for the extractive industries. *Miner. Econ.* **2021**, *35*, 221–237. [CrossRef]
94. KPMG Managing Risks of the Growing RPA Jungle. 2018. Available online: https://assets.kpmg/content/dam/kpmg/in/pdf/2018/12/Managing-risks-the-growing-RPA-jungle.pdf (accessed on 24 August 2021).
95. Schlarman, S. The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. *Inf. Syst. Secur.* **2001**, *10*, 1–6. [CrossRef]
96. Hunziker, S. Looking at Trends in ERM. *Enterp. Risk Manag. Mod. Approaches Balanc. Risk Reward.* **2019**, 209–234. [CrossRef]
97. Nicoletti, B. *Banking 5.0: How Fintech Will Change Traditional Banks in the 'New Normal' Post Pandemic*; Springer International Publishing: Cham, Switzerland, 2021. Available online: https://doi.org/10.1007/978-3-030-75871-4 (accessed on 5 September 2021).
98. FirstSource Extreme Automation for Business Process Management-The Next Normal. 2020. Available online: https://www.firstsource.com/blog/navigating-the-next-normal-with-extreme-automation (accessed on 5 September 2021).
99. Carden, L.L.; Maldonado, T.; Boyd, R.O. Organizational resilience. *Organ. Dyn.* **2018**, *47*, 25–31. [CrossRef]
100. Parise, G.; Martirano, L.; Parise, L. Electric Infrastructures Equalized to Strategic for Disaster Recovery in Emergencies. In Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Palermo, Italy, 12–15 June 2018; pp. 1–5. [CrossRef]
101. Gomez, G. What a Pandemic Teaches Us about Business Continuity and Efficiency. 28 July 2020. Available online: https://www.itproportal.com/features/what-a-pandemic-teaches-us-about-business-continuity-and-efficiency/ (accessed on 22 August 2021).
102. AiThority WAM Group Saves $1 Million and Maintains Business Continuity. 2020. Available online: https://aithority.com/robots/automation/wam-group-saves-1-million-and-maintains-business-continuity-with-automation-anywheres-saas-platform/ (accessed on 10 September 2022).
103. ElectroNeek. What Is RPA (Robotic Process Automation): An MSP Perspective. 2021. Available online: https://electroneek.com/blog/what-is-rpa-robotic-process-automation-an-msp-perspective/ (accessed on 10 September 2022).
104. Central, C. Using Intelligent Automation to Stay Ahead of COVID-19 Disruption. 2021. Available online: https://www.continuitycentral.com/index.php/news/resilience-news/6009-using-intelligent-automation-to-stay-ahead-of-covid-19-disruption (accessed on 1 August 2021).
105. DQINDIA. Leveraging Automation to Achieve Business Continuity for Insurers in the New Normal. 2020. Available online: https://www.dqindia.com/leveraging-automation-to-achieve-business-continuity-for-insurers-in-the-new-normal/ (accessed on 11 September 2022).
106. Pavlidis, G. Europe in the digital age: Regulating digital finance without suffocating innovation. *Law Innov. Technol.* **2021**, *13*, 464–477. [CrossRef]
107. ISACA. *COBIT 2019—Introduction and Methodology*; 2020; ISACA Volume 117. Available online: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC (accessed on 24 August 2021).
108. Introducing COBIT 2019—OVERVIEW November 2018. no. November, 2018. Available online: http://www.isaca.org/COBIT/Documents/COBIT-2019-Toolkitfmkeng1118.zip (accessed on 24 August 2021).
109. Nygård, A.R.; Katsikas, S. SoK: Combating threats in the digital supply chain. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Article no. 128. Vienna Austria, 23–26 August 2022; pp. 1–8. [CrossRef]
110. Chałubińska-Jentkiewicz, K. *Cybersecurity in Poland*; Springer: Cham, Switzerland, 2022. [CrossRef]
111. Alibasic, A.; Upadhyay, H.; Simsekler, M.C.E.; Kurfess, T.; Woon, W.L.; Omar, M.A. Evaluation of the trends in jobs and skill-sets using data analytics: A case study. *J. Big Data* **2022**, *9*, 1–28. [CrossRef]
112. FuturCIO IDC: 80% of FSIs in China to Use Intelligent Automation by 2023—FutureCIO. 2020. Available online: https://futurecio.tech/idc-80-of-fsis-in-china-to-use-intelligent-automation-by-2023/ (accessed on 10 September 2022).

113. Solis, B. COVID-19 Accelerates Enterprise Use of Automation in Digital Transformation. 2020. Available online: https://www.cio.com/article/193608/covid-19-accelerates-enterprise-use-of-automation-in-digital-transformation.html (accessed on 10 September 2022).
114. Fraser, J.; Simkins, B.J. Enterprise Risk Management. 2009. Available online: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118267080# (accessed on 27 December 2021).
115. Fukuyama, F. Governance: What Do We Know, and How Do We Know It? *Annu. Rev. Politi Sci.* **2016**, *19*, 89–105. [CrossRef]
116. Meriam-Webster Governance Definition & Meaning—Merriam-Webster. 2022. Available online: https://www.merriam-webster.com/dictionary/governance (accessed on 12 December 2021).
117. Biswas, A. Governance: Meaning, Definition, 4 Dimensions, and Types. 2020. Available online: https://schoolofpoliticalscience.com/definitions-and-types-of-governance/ (accessed on 12 December 2021).
118. McKinsey Industry 4.0: Reimagining Manufacturing Operations after COVID-19. 2020. Available online: https://www.mckinsey.com/business-functions/operations/our-insights/industry-40-reimagining-manufacturing-operations-after-covid-19 (accessed on 1 August 2021).
119. Shivakumar, S.K.; Build a Next-Generation Digital Workplace, B.N.-G.D. Available online: https://link.springer.com/book/10.1007/978-1-4842-5512-4 (accessed on 5 September 2021).
120. Orynbayeva, A. A Governance Model for Managing Robotics Process Automation (RPA). TU Delft—Faculty of Technology, Policy and Management, p. 78, 2019. Available online: https://repository.tudelft.nl/islandora/object/uuid%3Ab4609d10-9318-465c-baa4-e945e7de1a96 (accessed on 27 December 2021).
121. Asef-Sargent, J.; Lewis, A.C.; Everson, K.E.; Steinhoff, J.C. Put on Your Auditor Hat to Help Avoid Turbulence on the Intelligent Automation Journey. *Gov. Financ. Manag.* **2020**, *68*, 18–25. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=141939720&site=eds-live (accessed on 27 December 2021).
122. Sarangi, A.K.; Pradhan, R.P. ICT infrastructure and economic growth: A critical assessment and some policy implications. *Decision* **2020**, *47*, 363–383. [CrossRef]
123. Chambers, D.; Coronado, G.; Green, B.; Jarvik, J.; Septimus, E.; Tuzzio, L.; Zatzick, D. RPA Implementations: Key Considerations. 2017. Available online: https://www.pwc.in/assets/pdfs/publications/2018/rpa-implementation-key-considerations.pdf (accessed on 9 September 2021).
124. Ntansa How You Can Use RPA (Robotic Process Automation) to Enhance Your COVID19 Business Continuity Plan—Ntansa. June 2020. Available online: https://www.ntansa.com/how-you-can-use-rpa-robotic-process-automation-to-enhance-your-covid19-business-continuity-plan/ (accessed on 25 July 2021).
125. PwC Robotic Process Automation: A Primer for Internal Audit Professionals. PWC. 2018. pp. 1–4. Available online: https://www.pwc.com/sg/en/publications/assets/ra-robotic-process-automation-for-ia.pdf (accessed on 9 September 2021).
126. ISACA The Dark Side of Robotic Process Automation. 2020. Available online: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/the-dark-side-of-robotic-process-automation (accessed on 24 October 2021).
127. Church, K.S.; Schmidt, P.J.; Ajayi, K. Forecast Cloudy—Fair or Stormy Weather: Cloud Computing Insights and Issues. *J. Inf. Syst.* **2020**, *34*, 23–46. [CrossRef]
128. Chandler, S.; Power, C. Who minds the bots? PWC, p. 8, 2017. Available online: https://www.pwc.com.au/publications/assets/rpa-risk-controls.pdf (accessed on 9 September 2021).
129. Hubbard, T.; Fabius, J.A.; Steinhoff, J.C. Harnessing and Protecting Data Assets in a 21st Century Financial Enterprise. *J. Gov. Financ. Manag.* **2018**, *67*, 34–41. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=138653884&site=eds-live (accessed on 9 September 2021).
130. Islam, C.; Babar, M.A.; Nepal, S. A Multi-Vocal Review of Security Orchestration. *ACM Comput. Surv.* **2019**, *52*, 1–45. [CrossRef]
131. Hirschheim, R.; Heinzl, A.; Dibbern, J. (Eds.) *Information Systems Outsourcing: The Era of Digital Transformation*; Springer Nature Switzerland AG: Cham, Switzerland, 2020. [CrossRef]
132. Techwire Automate your Business Continuity Program with Resilience ONE by SAI Global—Tech Wire Asia. 2020. Available online: https://techwireasia.com/2019/07/automate-your-business-continuity-program-with-resilienceone-by-sai-global/ (accessed on 14 September 2021).
133. Hyland Is RPA Good for Information Security and Compliance? 2019. Available online: https://blog.hyland.com/content-services/compliance/is-rpa-good-for-information-security-and-compliance/ (accessed on 1 August 2021).
134. Kahan, D.; Oltmanns, A.; Kaczmarskyj, G.; Lamberton, C.; Gillard, A. Risk and Control Considerations within Robotic Process Automation Implementations Balancing Transformation with Risk Addressing History before It Repeats Itself. p. 12, 2018. Available online: https://engineering.report/Resources/Whitepapers/bceab695-0ac9-430c-ae6c-2fe8a4daa925_Risk-control-considerations-within-robotic-process-automation-implementations.pdf (accessed on 9 September 2021).
135. CIO Beyond Disaster Recovery: Intelligent Automation and Business Continuity. 2007. Available online: https://www.cio.com/article/2437417/beyond-disaster-recovery--intelligent-automation-and-business-continuity.html (accessed on 10 October 2021).
136. Butt, A.S. Mitigating the effects of COVID-19: An exploratory case study of the countermeasures taken by the manufacturing industry. *J. Bus. Ind. Mark.* **2021**, *ahead-of-print*. [CrossRef]
137. Workforce, D. Securing Business Continuity with RPA Maintenance. 2020. Available online: https://digitalworkforce.com/rpa-news/securing-business-continuity-with-rpa-maintenance/ (accessed on 25 July 2021).

138. Minnaar, D.; Smith, M. Internal Audit and Robotic Process Automation. pp. 1–16, 2018. Available online: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/intelligent-automation-and-internal-audit.pdf (accessed on 9 September 2021).
139. BCI The BCI Competency Framework. 2020. pp. 1–25. Available online: https://www.thebci.org/resource/bci-competency-framework.html (accessed on 9 September 2021).
140. Theuerkauf, J. Putting Your Business Continuity Plans in Motion, Phase Two: Industrializing Intelligent Automation. 2020. Available online: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/08/31/putting-your-business-continuity-plans-in-motion-phase-two-industrializing-intelligent-automation/?sh=842a3f6b3216 (accessed on 29 January 2022).
141. Met, İ.; Kabukçu, D.; Uzunoğulları, G.; Soyalp, Ü.; Dakdevir, T. Blending Business Strategies with IT in Digital Era in: Digital Business Strategies in Blockchain Ecosystems. 2020. Available online: https://link.springer.com/book/10.1007/978-3-030-29739-8 (accessed on 5 September 2021).
142. Saleem, J.; Hammoudeh, M.; Raza, U.; Adebisi, B.; Ande, R. IoT standardisation: Challenges, Perspectives and Solution. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, 26–27 June 2018. [CrossRef]
143. KPMG Ensuring Business Continuity Management Capabilities Case Study. 2020. Available online: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2020/03/robotic-process-automation-goes-hand-in-hand-with-you-to-tackle-a-crisis.pdf (accessed on 9 September 2021).
144. Patel, S. Bots Are the Future of Business Continuity. 22 April 2020. Available online: https://www.extratechnology.com/blog/bots-are-the-future-of-business-continuity (accessed on 14 September 2021).
145. Butterfield, W. The Promise of Automation in a Time of Crisis—The AI Journal. 2020. Available online: https://aijourn.com/the-promise-of-automation-in-a-time-of-crisis/ (accessed on 8 November 2021).
146. Rashid, A.N.M.B.; Ahmed, M.; Sikos, L.F.; Haskell-Dowland, P. Anomaly Detection in Cybersecurity Datasets via Cooperative Co-evolution-based Feature Selection. *ACM Trans. Manag. Inf. Syst.* **2022**, *13*, 1–39. [CrossRef]
147. Stojkovski, B.; Lenzini, G.; Koenig, V.; Rivas, S. What's in a Cyber Threat Intelligence sharing platform? In ACSAC 21: Annual Computer Security Applications Conference, pp. 385–398 2021. Available online: https://dl.acm.org/doi/10.1145/3485832.3488030 (accessed on 1 July 2021).
148. Ramanathan, N. Engineer's Perspective of the Future of Engineering Applications. Control Engineering. 2020. Volume 67, no. September. pp. 14–16. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=146014040&site=eds-live (accessed on 27 December 2021).
149. ECCI Automation in Business Continuity Management System. 2017. Available online: https://eccinternational.com/automation-business-continuity-management-system/ (accessed on 13 September 2021).
150. Mittal, M. RPA (Robotics Process Automation)—An Enabler of Business Continuity. 2020. Available online: https://www.linkedin.com/pulse/rpa-enabler-business-continuity-manish-mittal/ (accessed on 25 July 2021).
151. Matteson, S. How Robotic Process Automation Can Make Work More Efficient in Your Business—TechRepublic. 2021. Available online: https://www.techrepublic.com/article/how-robotic-process-automation-can-make-work-more-efficient-in-your-business/ (accessed on 8 November 2021).
152. Accenture A Resilient Future with Intelligent Automation. 2020. Available online: https://www.accenture.com/nl-en/blogs/insights/resilient-future-through-intelligent-automation (accessed on 1 August 2021).
153. Wu, W.-N. Organizational Resilience: Examining the Influence of Information Cost and Organizational Capacity on Business Continuity Management. In *HCI in Business, Government and Organizations. HCII 2021. Lecture Notes in Computer Science (LNISA)*; Springer: Cham, Switzerland, 2021. [CrossRef]
154. Loke, S.W.; Rakotonirainy, A. An Overview of Technology Trends towards Smarter Cities. In *The Automated City: Internet of Things and Ubiquitous Artificial Intelligence*; no. April; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 1–4. [CrossRef]
155. Sameer Kishore Adopt the New Normal. Milestone Technologies. No. August. 2020. Available online: https://www.siliconindia.com/vendor/milestone-technologies-adopt-the-new-normal-cid-3601.html (accessed on 24 August 2021).
156. Ellitan, L.; Anatan, L. International Journal of Trend in Scientific Research and Development (IJTSRD) Achieving Business Continuity in Industrial 4.0 and Society 5.0. *Int. J. Trend Sci. Res. Dev.* **2020**, *2*, 1–5.
157. Ward-Dutton, N. From RPA to DPA: A Strategic Approach to Automation. MWD Advisors. 2018. Available online: https://www.pega.com/system/files/resources/2018-12/from-rpa-to-dpa.pdf (accessed on 24 August 2021).
158. Spring, J.M.; Illari, P. Review of Human Decision-making during Computer Security Incident Analysis. *Digit. Threat. Res. Pr.* **2021**, *2*, 1–47. [CrossRef]
159. TP&P Robotic Process Automation (RPA) Post Implementation: How to Scale Effectively? 2020. Available online: https://www.tpptechnology.com/blog/robotic-process-automation-rpa-post-implementation-how-to-scale-effectively/ (accessed on 11 October 2021).
160. Lanz, B.J.; Sussman, B.I. Program Management in a COVID-19 World. *CPA J.* **2020**, *90*, 28–35.
161. Schneider, F.; Weiller, C. Big Data und künstliche Intelligenz. *Der Nervenarzt* **2018**, *89*, 859–860. [CrossRef] [PubMed]
162. Commission, E. EUR-Lex-52020PC0595-EN-EUR-Lex. 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595 (accessed on 12 September 2022).

163. Vosmeer, L. Digital Operational Resilience Act: The Enhancement of Digital Resilience in EU's Financial Sector. 2022. Available online: https://www.cgi.com/sites/default/files/2022-10/cgi-dora-en.pdf (accessed on 21 November 2022).
164. Ahern, D. Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon. *Eur. Bus. Organ. Law Rev.* **2021**, *22*, 395–432. [CrossRef]
165. Assentian, I.D.; Aranda, N.I. Overview of Applicable Regulations in Digital Finance and Supporting Technologies. *Big Data Artif. Intell. Digit. Financ.* **2022**, 337–351. [CrossRef]
166. Mahajan, R.; Kaliyamurthy, S.; Gupte, A.; Sharma, A.; Parthasarathy, S.; Godbole, P.; Crasto, A. Risk Management for and by the BOT. Deloitte Publication. 2018. Available online: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-bot-risk-management-noexp.pdf (accessed on 24 August 2021).
167. Farhat, I.I. Rpa and the Gouernment Audit. *J. Gov. Financ. Manag.* **2019**, *68*, 42–47. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=136473213&site=eds-live (accessed on 27 December 2021).
168. Knowledge Risk Management. Durst, S.; Henschel, T. (Eds.) 2020. Available online: https://link.springer.com/book/10.1007/978-3-030-35121-2 (accessed on 5 September 2021).
169. Pedroza, G.V. New Trends in Organizational Resilience and Business Continuity. 2022. Available online: https://drj.com/journalmain/new-trends-in-organizational-resilience-and-business-continuity/ (accessed on 10 September 2022).
170. Syed, R.; Suriadi, S.; Adams, M.; Bandara, W.; Leemans, S.J.; Ouyang, C.; ter Hofstede, A.H.; van de Weerd, I.; Wynn, M.T.; Reijers, H.A. Robotic Process Automation: Contemporary themes and challenges. *Comput. Ind.* **2019**, *115*, 103162. [CrossRef]
171. Infosys Security Considerations in Robotic Process Automation. 2020. Available online: https://www.infosys.com/services/cyber-security/documents/rpa-security.pdf (accessed on 24 August 2021).
172. Santos, H.; Oliveira, A.; Soares, L.; Satis, A.; Santos, A. Information Security Assessment and Certification within Supply Chains. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Article No.: 135. Vienna, Austria, 17–20 August 2021; pp. 1–6. [CrossRef]
173. Ye, D.; Liu, M.J.; Luo, J.; Yannopoulou, N. How to Achieve Swift Resilience: The Role of Digital Innovation Enabled Mindfulness. *Inf. Syst. Front.* **2022**, 1–23. [CrossRef]
174. KPMG Ensuring Business Continuity Management Capabilities Robotic Process Automation (RPA) Goes Hand-in-Hand. 2020. Available online: https://vdocument.in/ensuring-business-continuity-management-capabilities-robotic-process-automation.html (accessed on 14 November 2021).
175. Unhelkar, B.; Gonsalves, T. Enhancing Artificial Intelligence Decision Making Frameworks to Support Leadership During Business Disruptions. *IT Prof.* **2020**, *22*, 59–66. [CrossRef]
176. Rashid, N.; Zumerle, D.; Tornbohm, C. Four Steps to Ensure Robotic Process Automation Security. Gartner. No. January. 2021. pp. 1–9. Available online: https://www.gartner.com/document/3995635?ref=solrAll&refval=290482844 (accessed on 24 August 2021).
177. Bovaird, V.; Kundu, S.; Moir, J.; Sanmugananthan, S.; Turk, D. Automation Is Here to Stay but What about Your Workforce? Preparing Your Organization for the New Worker Ecosystem. Deloitte. 2017. pp. 1–17. Available online: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-automation-here-to-stay.pdf (accessed on 24 August 2021).
178. Health, E. How to Maximize People Power with Digital Capabilities. No. November. 2020. pp. 14–16. Available online: https://www.plantengineering.com/articles/how-to-maximize-people-power-with-digital-capabilities/ (accessed on 24 August 2021).
179. Jolly, R. Digital BCP Business Continuity Plan Is Your Organization COVID Ready. 2020. Available online: https://www.techmahindra.com/en-in/blog/digital-bcp-business-continuity-plan-is-your-organization-covid-ready/ (accessed on 5 September 2021).
180. Alam, N.; Gupta, L.; Zameni, A. *Fintech and Islamic Finance*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019. [CrossRef]
181. Banker, S. Automation Is the Future of Warehousing. Forbes. No. August. 2020. pp. 4–6. Available online: https://www.forbes.com/sites/stevebanker/2020/07/31/automation-is-the-future-of-warehousing/#336140ba30f4 (accessed on 24 August 2021).
182. McKinsey The Next S-Curve in Model Risk Management. The Next S-Curve in Model Risk Management. 2021. Available online: https://www.mckinsey.com/business-functions/risk/our-insights/the-next-s-curve-in-model-risk-management (accessed on 24 August 2021).
183. CloudOak. Five Benefits of Automating Your Business Continuity Plan. 2017. Available online: https://www.cloudoakchannel.com/five-benefits-of-automating-your-business-continuity-plan/ (accessed on 13 September 2021).
184. Mitratech. How Workflow Automation Builds Business Continuity After COVID-19. 2020. Available online: https://mitratech.com/resource-hub/blog/workflow-automation-business-continuity-covid-19/ (accessed on 13 September 2021).
185. Hodge, B. Why 'Operationalizing RPA' Is the Right Solution for SSOs in the Philippines. 2017. Available online: https://www.ssonetwork.com/rpa/whitepapers/why-operationalizing-rpa-is-the-right-solution (accessed on 24 August 2021).
186. Reciprocity Compliance Considerations for Robotic Process Automation. 2021. Available online: https://reciprocity.com/compliance-considerations-for-robotic-process-automation/ (accessed on 7 November 2021).

187. Propelex Managing Risk with Robust Business Continuity & Disaster Recovery Services and Solutions. 2021. Available online: https://www.propelex.com/wp-content/uploads/2021/06/Business-Continuity-Disaster-Recovery-RPA-Startup-Case-Study-Propelex-BCDR.pdf (accessed on 10 September 2022).
188. Suyati How Businesses can Leverage RPA to Emerge Stronger after a Crisis. 2022. Available online: https://suyati.com/blog/rpa-can-help-your-business-emerge-stronger-after-covid-19/ (accessed on 24 August 2021).
189. QuickReach 5 Benefits of Ensuring Business Continuity via Intelligent Automation. 2020. Available online: https://www.youtube.com/watch?v=aXhKD4KBMWA (accessed on 5 September 2021).
190. Goodchild, J. Rise of the Robots: How You Should Secure RPA. 2020. Available online: https://www.darkreading.com/edge-articles/rise-of-the-robots-how-you-should-secure-rpa (accessed on 10 October 2021).
191. McKinsey Global Institute. *Overcoming Obesity: An initial Economic Analysis*; McKinsey & Company: London, UK, 2014.
192. Sheikhattar, M.R.; Nezafati, N.; Shokouhyar, S. A thematic analysis–based model for identifying the impacts of natural crises on a supply chain for service integrity: A text analysis approach. *Environ. Sci. Pollut. Res.* **2022**, *29*, 79413–79433. [CrossRef]
193. Marcucci, G.; Antomarioni, S.; Ciarapica, F.E.; Bevilacqua, M. The impact of Operations and IT-related Industry 4.0 key technologies on organizational resilience. *Prod. Plan. Control* **2021**, *33*, 1417–1431. [CrossRef]
194. Hald, K.S.; Coslugeanu, P. The preliminary supply chain lessons of the COVID-19 disruption—What is the role of digital technologies? *Oper. Manag. Res.* **2021**, *15*, 282–297. [CrossRef]
195. Rau, R.; Wardrop, R.; Zingales, L. (Eds.) Palgrave Macmillan Cham. In *The Palgrave Handbook of Technological Finance*; 2021. Available online: https://link.springer.com/book/10.1007/978-3-030-65117-6 (accessed on 5 September 2021).
196. McCuen, R.H. Book Reviews. *JAWRA J. Am. Water Resour. Assoc.* **2011**, *47*, 650–653. [CrossRef]
197. Modgil, S.; Singh, R.K.; Hannibal, C. Artificial intelligence for supply chain resilience: Learning from COVID-19. *Int. J. Logist. Manag.* **2021**, *33*, 1246–1268. [CrossRef]
198. Agnihotri, R. Autonomous Operations in Process Manufacturing—Part 2. no. October, 2020. pp. 11–16. Available online: https://www.hydrocarbonprocessing.com/magazine/2020/october-2020/trends-and-resources/business-trends-autonomous-operations-in-process-manufacturing-part-2 (accessed on 24 August 2021).
199. Conway, E.; Byrne, D. Contemporary Issues in Accounting. 2018. Available online: https://link.springer.com/book/10.1007/978-3-319-91113-7 (accessed on 5 September 2021).
200. Carden, L.; Maldonado, T.; Brace, C.; Myers, M. Robotics process automation at TECHSERV: An implementation case study. *J. Inf. Technol. Teach. Cases* **2019**, *9*, 72–79. [CrossRef]
201. Mohanty, S.; Vyas, S. Intelligent Process Automation = RPA + AI. In *How to Compete in the Age of Artificial Intelligence*; Apress: Berkeley, CA, USA, 2018; pp. 125–141. [CrossRef]
202. Soldatos, J.; Kefalakis, N.; Makantasis, G.; Marguglio, A.; Lazaro, O. Digital Platform and Operator 4.0 Services for Manufacturing Repurposing During COVID19. In *Advances in Production Management Systems. Artificial Intelligence for Sustainable and Resilient Production Systems: IFIP WG 5.7 International Conference, APMS 2021, Nantes, France, September 5–9, 2021, Proceedings, Part IV*; Springer International Publishing: Cham, Switzerland, 2021; Volume 633, pp. 311–320. Available online: https://link.springer.com/chapter/10.1007/978-3-030-85910-7_33 (accessed on 5 September 2021).
203. Sherringham, K.; Unhelkar, B. (Eds.) *Crafting and Shaping Knowledge Worker Services in the Information Economy*; Palgrave Macmillan: Singapore, 2020; pp. 147–159. [CrossRef]
204. Gopisetty, S. Global Pandemic: Business Model Impact on Enterprises reTHINK, reIMAGINE, reINVENT Businesses. In Proceedings of the 2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI), Atlanta, GA, USA, 28–31 October 2020; pp. 114–120. [CrossRef]
205. Harrast, S.A. Robotic process automation in accounting systems. *J. Corp. Account. Financ.* **2020**, *31*, 209–213. [CrossRef]
206. Nicoletti, B. *Procurement 4.0 and the Fourth Industrial Revolution: The Opportunities and Challenges of a Digital World*; Palgrave Macmillan: Cham, Switzerland, 2020; Volume 13. [CrossRef]
207. BCI. BCM Legislations, Regulations, Standards and Good Practice. 2020. Available online: https://www.thebci.org/resource/bcm-legislations--regulations--standards-and-good-practice.html (accessed on 13 March 2021).
208. ECM, T. How Low Code Can Supercharge Digital Transformation? 2021. Available online: https://theecmconsultant.com/what-is-low-code/ (accessed on 14 November 2021).
209. Devi, O.R. Disruptive emerging technologies: Change in service operating model. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *4*, 15–21.
210. Senna, P.; Reis, A.; Santos, I.L.; Dias, A.C.; Coelho, O. A systematic literature review on supply chain risk management: Is healthcare management a forsaken research field? *Benchmarking: Int. J.* **2020**, *28*, 926–956. [CrossRef]
211. Delany, C. Kangaroo Court: Robotic Process Automation. 2021. Available online: https://www.jdsupra.com/legalnews/kangaroo-court-robotic-process-7974558/ (accessed on 8 September 2021).
212. Susilo, A.; Prabowo, H.; Kosasih, W.; Kartono, R.; Tjhin, V.U. The Implementation of Robotic Process Automation for Banking Sector Case Study of a Private Bank in Indonesia. In Proceedings of the 9th International Conference on Information Technology: IoT and Smart City, Guangzhou, China, 22–25 December 2021; pp. 365–371. [CrossRef]
213. Lamid, L.I.; Ibrahim, I.A.; Abdullahi, K.I.; Abdullahi, U.G. A Framework for Digital Government Transformation Performance Assessment and Toolkit for Developing Countries. In Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance, Athens, Greece, 6–8 October 2021; pp. 203–215. [CrossRef]

214. Stevens, R.; Votipka, D.; Dykstra, J.; Tomlinson, E.; Quartararo, E.; Ahern, C.; Mazurek, M.L. How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, New Orleans, LA, USA, 29 April–5 May 2022; Article No.: 589, pp. 1–18. [CrossRef]
215. Zhang, L.; Fang, X.; Chen, Y.; Song, Y.; Qian, S. Research on business continuity rating model in cloud environment. In Proceedings of the 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference, Chongqing, China, 12–14 March 2021; Volume 5, pp. 1702–1705. [CrossRef]
216. Muthoni, S.; Okeyo, G.; Chemwa, G. Infrastructure as Code for Business Continuity in Institutions of Higher Learning. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies, Cape Town, South Africa, 9–10 December 2021; pp. 1–6. [CrossRef]
217. Mooshian, C. How to Choose Which RPA/Intelligent Automation Platform Is Right for You. 2021. Available online: https://www.informationweek.com/big-data/how-to-choose-which-rpa-intelligent-automation-platform-is-right-for-you (accessed on 6 September 2022).
218. Seele, P.; Schultz, M.D. From Greenwashing to Machinewashing: A Model and Future Directions Derived from Reasoning by Analogy. *J. Bus. Ethic-* **2022**, *178*, 1063–1089. [CrossRef]
219. MouriTech Robotic Process Automation | Smart Processes. 2022. Available online: https://www.mouritech.com/it-services-solutions/automation/robotic-process-rpa/ (accessed on 10 September 2022).
220. InfoFort Robotic Process Automation. 2022. Available online: https://www.infofort.com/solutions/RPA.aspx (accessed on 10 September 2022).
221. Scsp Values of Automation for Business Continuity | Safety Consultants & Solution Provider. 2022. Available online: https://scspng.com/blog/values-of-automation-for-business-continuity (accessed on 10 September 2022).
222. IDC IDC Predicts 80% of Financial Services Institutions in China Will Deploy Intelligent Automation Solutions by 2023. 2020. Available online: https://www.idc.com/getdoc.jsp?containerId=prAP46575520 (accessed on 30 July 2021).
223. Agarwal, S.; Bhardwaj, G.; Saraswat, E.; Singh, N.; Aggarwal, R.; Bansal, A. Insurtech Fostering Automated Insurance Process using Deep Learning Approach. In Proceedings of the 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India, 23–25 February 2022; Volume 2, pp. 386–392. [CrossRef]
224. Edeline, K.; Carlisi, T.; Iurman, J.; Donnet, B. Towards a Closed-Looped Automation for Service Assurance with the D X A GENT. In *2022 2nd International Workshop on Intent-based Networking*; IEEE: Piscataway, NJ, USA, 2022; pp. 67–72. Available online: https://ieeexplore.ieee.org/document/9844116 (accessed on 14 June 2021).
225. Curry, E.; Auer, S.; Berre, A.J.; Metzger, A.; Perez, M.S.; Zillner, S. Technologies and Applications for Big Data Value. In *Technologies and Applications for Big Data Value*; Springer: Cham, Switzerland, 2022; pp. 1–15. [CrossRef]
226. Anywhere, A. RPA & Automation for Business Continuity. 2021. Available online: https://www.automationanywhere.com/solutions/rpa-business-continuity (accessed on 25 July 2021).
227. Liao, X. Why Automation Will Be Critical for Business Continuity Post-Pandemic. 1 June 2020. Available online: https://www.joltag.com/blog/why-automation-will-be-critical-for-business-continuity-post-pandemic (accessed on 25 July 2021).
228. Uniphore Key Highlights of Intelligent Automation APAC Summit 2021. 2021. Available online: https://www.uniphore.com/key-highlights-of-intelligent-automation-apac-summit-2021 (accessed on 5 September 2021).
229. Emergence How Intelligent (and Integrated) Automation Can Build Resilience in the New Normal. 2020. Available online: https://emergencehq.com/how-intelligent-and-integrated-automation-can-build-resilience-in-the-new-normal/ (accessed on 5 September 2021).
230. AI, C. Is AI Part of Your Business Continuity Plan? 2020. Available online: https://www.chisel.ai/blog/is-ai-part-of-your-business-continuity-plan (accessed on 5 September 2021).
231. Cyber, R. Intelligent Mortgage Processing with RPA&ML. 2020. Available online: https://www.royalcyber.com/resources/webcasts/intelligent-mortgage-processing-with-rpa-and-ml/ (accessed on 5 September 2021).
232. Associates, T. Intelligent Automation: Three Questions to Achieve Immediate Impact and Prepare for the Future. 2021. Available online: https://www.tofflerassociates.com/vanishing-point/intelligent-automation-three-questions-to-achieve-immediate-impact-and-prepare-for-the-future (accessed on 5 September 2021).
233. BackBox. How AI Technologies Can Assist You with Post-Disaster Business Continuity. 2021. Available online: https://backbox.com/how-ai-technologies-can-assist-you-with-post-disaster-business-continuity/ (accessed on 24 August 2021).
234. Informa Ensuring Business Continuity with Artificial Intelligence. 2020. Available online: https://aibusiness.com/author.asp?sectionid=789&docid=761245 (accessed on 29 January 2022).
235. Comidor Using Intelligent Process Automation to Build Business Resiliency. 2021. Available online: https://www.comidor.com/wp-content/uploads/2021/06/intelligent-automation-report-June-2021.pdf (accessed on 24 August 2021).
236. DUCO How To Make Intelligent Process Automation (IPA) A Reality. 2020. Available online: https://du.co/how-to-make-intelligent-process-automation-ipa-a-reality/ (accessed on 1 November 2021).
237. Capgemini Intelligent Process Automation. 2020. Available online: https://www.capgemini.com/resources/intelligent-process-automation/ (accessed on 24 August 2021).
238. Vanner, C. 3 Ways Process Automation Can Aid Your Business Recovery. 17 September 2020. Available online: https://www.bizagi.com/en/blog/digital-process-automation/3-ways-process-automation-can-aid-your-business-recovery (accessed on 25 July 2021).

239. Partners, S. What is Intelligent Automation? Four Business Drivers. 2021. Available online: https://sdlcpartners.com/insights/what-is-intelligent-automation/ (accessed on 1 August 2021).
240. Informed, B.I. COVID-19 as a Catalyst for Digital Innovation. 2020. Available online: https://www.beinformed.com/blog/covid-19-as-a-catalyst-for-digital-innovation/ (accessed on 7 November 2021).
241. Cappadoro-Moss, T. Customer Lifecycle Management—The Journey to AI—Led Automation. 2021. Available online: https://www.workfusion.com/blog/customer-lifecycle-management-the-journey-to-ai-led-process-automation/ (accessed on 7 November 2021).
242. Pansare, R.; Yadav, G. Repurposing production operations during COVID-19 pandemic by integrating Industry 4.0 and reconfigurable manufacturing practices: An emerging economy perspective. *Oper. Manag. Res.* **2022**, *15*, 1270–1289. [CrossRef]
243. Sastararuji, D.; Hoonsopon, D.; Pitchayadol, P.; Chiwamit, P. Cloud accounting adoption in Thai SMEs amid the COVID-19 pandemic: An explanatory case study. *J. InNovember Entrep.* **2022**, *11*, 1–25. [CrossRef]
244. Naik, B.; Mehta, A.; Yagnik, H.; Shah, M. The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex Intell. Syst.* **2021**, *8*, 1763–1780. [CrossRef]
245. Popchev, I.; Radeva, I.; Velichkova, V. The impact of blockchain on internal audit. In Proceedings of the 2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE), Sofia, Bulgaria, 28–29 October 2021; pp. 1–8. [CrossRef]
246. Griffioen, A. Robotic Process Automation (RPA) in Financial Services | 360 Managed. 2019. Available online: https://www.360managed.com.au/rpa-in-financial-services/ (accessed on 10 September 2022).
247. Sobczak, A. Robotic Process Automation as a Digital Transformation Tool for Increasing Organizational Resilience in Polish Enterprises. *Sustainability* **2022**, *14*, 1333. [CrossRef]
248. Samans, R.; Nelson, J. *Sustainable Enterprise Value Creation: Implementing Stakeholder Capitalism through Full ESG Integration*; Palgrave Macmillan: Cham, Switzerland, 2022; pp. 1–289. [CrossRef]
249. Bots, C. 11 Myths about Robotic Process Automation. 2018. Available online: https://cfb-bots.medium.com/11-myths-about-robotic-process-automation-b3bb019263fd (accessed on 10 September 2022).
250. Biffl, S.; Gerhard, D.; Lüder, A. *Multi-Disciplinary Engineering for Cyber-Physical Production Systems: Data Models and Software Solutions for Handling Complex Engineering Projects*; Springer: Cham, Switzerland, 2017; p. XII-472. Available online: https://link.springer.com/book/10.1007/978-3-319-56345-9 (accessed on 5 September 2021).
251. Brás, J.; Guerreiro, S. DEMO Business Processes Design to Improve the Enterprise Business Continuity Plans. In *Advances in Enterprise Engineering XI. EEWC 2017. Lecture Notes in Business Information Processing*; Springer: Cham, Switzerland, 2017; Volume 284, pp. 99–107. [CrossRef]
252. Bonichon, R.; Canet, G.; Correnson, L.; Goubault, É.; Haucourt, E.; Hirschowitz, M.; Labbé, S.; Mimram, S.; Flammini, F.; Bolonha, S.; et al. BACRank: Ranking Building Automation and Control System Components by Business Continuity Impact. In *Computer Safety, Reliability, and Security. 38th International Conference, SAFECOMP 2019, Turku, Finland, 11–13 September 2019, Proceedings 38*; Springer International Publishing: Cham, Switzerland, 2019; Volume 6894. Available online: https://link.springer.com/chapter/10.1007/978-3-030-26601-1_13#citeas (accessed on 5 September 2021).
253. Goswami, S. Applying Automation to Business Continuity Planning. 2020. Available online: https://www.bankinfosecurity.asia/applying-automation-to-business-continuity-planning-a-15411 (accessed on 13 September 2021).
254. Intive Leveraging Information-Based Analytics and Intelligent Automation. An Interview with Kannan Janardhanan. 2021. Available online: https://intive.com/insights/leveraging-information-based-analytics-and-intelligent-automation-an (accessed on 5 September 2021).
255. Anywhere, A. The Next Step for Business Continuity. 2020. Available online: https://www.automationanywhere.com/company/blog/rpa-thought-leadership/top-it-investments-for-business-continuity (accessed on 1 August 2021).
256. Automation, G. How to Automate Your Business Continuity Plan. 2017. Available online: http://www.genieautomation.com/how-to-automate-your-business-continuity-plan/ (accessed on 13 September 2021).
257. Bristow, E. 10 Questions to Answer in Your RPA Business Continuity Plans. 14 September 2020. Available online: https://www.linkedin.com/pulse/10-questions-answer-your-rpa-business-continuity-plans-emily-bristow/ (accessed on 14 September 2021).
258. Al-Essa, H.A.; Al-Sharidah, A.H. An Approach to Automate Business Impact Analysis. In Proceedings of the 2018 IEEE International Systems Engineering Symposium (ISSE), Rome, Italy, 1–3 October 2018; pp. 1–3. [CrossRef]
259. techUK Simplifying the Automation Conversation. 2021. Available online: https://www.techuk.org/resource/simplifying-the-automation-conversation.html (accessed on 5 September 2021).
260. Mesquita, A.; Camarinha, A.P.; Lopes, F.C.; Malta, P. What Will the Future of Work Look Like for IS Professionals? The Picture of Portugal. In *The Future of Digital Work: The Challenge of Inequality. IFIPJWC 2020. IFIP Advances in Information and Communication Technology*; Bandi, R.K., Klein, S., Madon, S., Monteiro, E., Eds.; Springer: Cham, Switzerland, 2020; Volume 601, pp. 341–358. [CrossRef]
261. Datafloq Chatbots and Intelligent Automation Solutions Paving the Way towards Seamless Business Continuity. 2020. Available online: https://datafloq.com/read/chatbots-intelligent-automation-solutions-paving-way-towards-seamless-business-continuity/8850 (accessed on 5 September 2021).
262. Zinnov Hyper Intelligent Automation—Accelerating Business Resiliency during COVID-19. 2020. Available online: https://zinNovembercom/hyper-intelligent-automation-accelerating-business-resiliency-during-covid-19/ (accessed on 5 September 2021).

263. Malek, R.T.F.F.B.P.A.A.R.J.L.H. Intelligent Framework for Business Process Automation and Re-Engineering. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 624–629. Available online: https://dl.acm.org/doi/abs/10.1109/IS.2018.8710523 (accessed on 1 July 2021).
264. HCL Intelligent Automation in the Battle against COVID-19 and Securing Business Continuity for the Future. 2020. Available online: https://www.hcltech.com/blogs/intelligent-automation-battle-against-covid-19-and-securing-business-continuity-future (accessed on 14 September 2021).
265. FirstPost. Automation to Drive Business Continuity, Efficiency and Value Addition from Human Resources—Technology News. 2020. Available online: https://www.firstpost.com/tech/news-analysis/automation-to-drive-business-continuity-efficiency-and-value-addition-from-human-resources-9059131.html (accessed on 14 September 2021).
266. Srivastava, S. COVID-19 Proves the Worth of Intelligent Automation for Business Continuity. Analytics Insight. 2020. Available online: https://www.analyticsinsight.net/covid-19-proves-worth-intelligent-automation-business-continuity/ (accessed on 14 September 2021).
267. Williams, J. Robotic Process Automation in the Fight against COVID-19: Part 4—Banking, Financial Services, and Insurance—Hyperautomation World. 2020. Available online: https://hyperautomation.world/covid-19/rpa-in-the-fight-against-covid-19-part-4-banking-finance-insurance/ (accessed on 1 November 2021).
268. Theuerkauf, J. Rethinking Business Continuity and Disaster Recovery Planning with Automation. Forbes. 19 June 2021. Available online: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/01/14/rethinking-business-continuity-and-disaster-recovery-planning-with-automation/?sh=41205787aded (accessed on 25 July 2021).
269. RICS Business Continuity & Resilience: Rebooting the Workplace. 2020. Available online: https://www.rics.org/east-asia/training-events/cpd/cpd-foundation-on-demand/cpd-foundation-on-demand-content/business-continuity-resilience-rebooting-the-workplace/ (accessed on 5 September 2021).
270. Hohli, P. Delivering Business Continuity with Intelligent Automation. 2021. Available online: https://straighttalk.hcltech.com/blogs/delivering-business-continuity-with-intelligent-automation (accessed on 25 November 2021).
271. Grzelak, M. Benefits of Robotic Process Automation. 2021. Available online: https://dtmates.com/en/automation/robotic-process-automation-benefits/ (accessed on 7 November 2021).
272. Magazine, B. How to Choose Between Robotic Process Automation & Financial Close Automation. 2021. Available online: https://www.blackline.com/blog/how-to-choose-rpa-financial-close-automation/ (accessed on 10 August 2021).
273. Carter, S. Automation in Business: Why It Matters and Why Your Organisation Needs It. Towards Data Science. 2021. Available online: https://towardsdatascience.com/automation-in-business-why-it-matters-and-why-your-organisation-needs-it-9ca2162ee204 (accessed on 6 August 2021).
274. Group, H. Robotic Process Automation: An Essential Co-worker for the Digital Age. 2021. Available online: https://blog.thehcigroup.com/robotic-process-automation-an-essential-co-worker-for-the-digital-age (accessed on 5 October 2021).
275. Butcher, S. RPA and Talent the Key to Powering Businesses. 2020. Available online: https://itbrief.com.au/story/rpa-and-talent-the-key-to-powering-businesses (accessed on 5 July 2021).
276. Julka, S. What Is Robotic Process Automation (RPA) ? Ultimate Guide to RPA and How It's Driving Digital Transformation? 2021. Available online: https://www.nseit.com/resources/blogs/robotic-process-automation-ultimate-guide (accessed on 7 June 2021).
277. Mirzazadeh, M. Process Automation & Business Continuity: How to Operate Efficiently. 2021. Available online: https://wave-tsg.com/process-automation-business-continuity-how-to-operate-efficiently/ (accessed on 8 November 2021).
278. Forbes from Eventually to Immediately: Continuity Is the Major Reason Automation Can't Wait. 2020. Available online: https://www.forbes.com/sites/forbestechcouncil/2020/12/02/from-eventually-to-immediately-continuity-is-the-major-reason-automation-cant-wait/?sh=4ac47f643036 (accessed on 7 November 2021).
279. Capgemini Being Recession Ready: Levering Intelligent Automation to Instil Operational Resilience. 2021. Available online: https://www.capgemini.com/gb-en/2021/06/being-recession-ready-levering-intelligent-automation-to-instil-operational-resilience/ (accessed on 7 November 2021).
280. Perpetuuiti Automation Simplified. 2021. Available online: https://www.ptechnosoft.com/iResiliencyAutomation.php (accessed on 7 November 2021).
281. William, J. How to Bring a Culture of Automation into Your Organization. Forbes. 2021. Available online: https://www.forbes.com/sites/forbesbusinesscouncil/2021/02/10/how-to-bring-a-culture-of-automation-into-your-organization/?sh=ef0853b7c656 (accessed on 8 November 2021).
282. Kadam, H. Robotic Process Automation Sweeps Across the Healthcare Industry. 2021. Available online: https://www.electronicdesign.com/industrial-automation/article/21168890/global-market-insights-robotic-process-automation-sweeps-across-the-healthcare-industry (accessed on 8 November 2021).
283. Rosner, C. BPA vs. RPA vs. RDA, Oh My! Here are the Differences and Similarities. 2021. Available online: https://www.ttec.com/blog/bpa-vs-rpa-vs-rda-oh-my-here-are-differences-and-similarities (accessed on 8 November 2021).
284. Hanna, T. The 15 Best Business Continuity Software and Tools to Consider for 2021. 2021. Available online: https://solutionsreview.com/backup-disaster-recovery/the-best-business-continuity-software-and-tools/ (accessed on 8 November 2021).
285. Weiss, D. Accelerate Business Continuity with Automated Backups. 2021. Available online: https://www.datto.com/blog/accelerate-business-continuity-with-automated-backups (accessed on 8 November 2021).

286. Westlake, J. Business Continuity Software—A Major Asset to Business Continuity Planning. 2021. Available online: https://www.globalapptesting.com/blog/business-continuity-planning-software-release (accessed on 8 November 2021).
287. Chakray Business Automation | Intelligent Automation Service & Solution. 2021. Available online: https://www.chakray.com/initiatives/business-automation/ (accessed on 8 November 2021).
288. Ciraldo, J. Best Business Continuity Tools That Create Organizational Resilience. 2021. Available online: https://www.beekeeper.io/blog/business-continuity-software-tools/ (accessed on 8 November 2021).
289. Forbes Improving Business Resilience in Challenging Times: Top Five Technologies to Invest In. 2021. Available online: https://www.forbes.com/sites/forbestechcouncil/2021/10/18/improving-business-resilience-in-challenging-times-top-five-technologies-to-invest-in/?sh=c9d0f8569f6f (accessed on 4 November 2021).
290. UiPath UiPath Brings Best-in-Class UI and API Automation Together and Strengthens Enterprise Scale in 2021.10 Platform Release. 2021. Available online: https://www.uipath.com/newsroom/uipath-brings-best-in-class-ui-and-api-automation-together (accessed on 14 November 2021).
291. ElectroNeek Automation in BCDR: How ElectroNeek RPA Can Help MSPs. 2021. Available online: https://electroneek.com/blog/rpa-for-msps/automation-in-bcdr-how-electroneek-rpa-can-help-msps/ (accessed on 11 October 2021).
292. Jones, M. RPA—the Short and Long-Term Solution to Business Continuity? 2020. Available online: https://techhq.com/2020/07/rpa-the-short-and-long-term-solution-to-business-continuity/ (accessed on 25 July 2021).
293. Fiaidhi, J.; Mohammed, S.; Mohammed, S. *Pragmatic Interoperability for Extreme Automation and Healthcare Interoperability and Continuity*; Springer: Singapore, 2021.
294. Schuler, J.; Gehring, F. Implementing Robust and Low-Maintenance Robotic Process Automation (RPA) Solutions in Large Organisations. *SSRN Electron. J.* **2019**, 1–29. [CrossRef]
295. Truong, H.-L.; Zhang, L. Resilience and Elasticity for Continuous Service-Based Processes in Pandemic Ages. *IT Prof.* **2021**, *23*, 31–37. [CrossRef]
296. Rauch, E.; Vickery, A.R.; Brown, C.A.; Matt, D.T. SME Requirements and Guidelines for the Design of Smart and Highly Adaptable Manufacturing Systems. In *Industry 4.0 for SMEs: Challenges, Opportunities and Requirements*; Matt, D.T., Modrák, V., Zsifkovits, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 39–72. [CrossRef]
297. How to Optimize Your Intelligent Automation Build. 2020. Available online: https://www.ey.com/enbe/financial-services/how-to-optimize-your-intelligent-automation-build (accessed on 5 September 2021).
298. Consulting, vs. Session 08—Business Continuity Powered by AI and Automation. 2020. Available online: https://www.youtube.com/watch?v=rWVchFNcw34 (accessed on 13 September 2021).
299. Sookoo, A.; Garg, L.; Chakraborty, C. Improvement of system performance in an IT production support environment. *Int. J. Syst. Assur. Eng. Manag.* **2021**, *12*, 461–479. [CrossRef]
300. Păunescu, C. How prepared are Small and Medium Sized companies for BCM ? *Qual. Access Success* **2017**, *18*, 1–6.
301. Aleksandrova, S.V.; Aleksandrov, M.N.; Vasiliev, V.A. Business Continuity Management System. In Proceedings of the 2018 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), St. Petersburg, Russia, 24–28 September 2018; pp. 14–17. [CrossRef]
302. ISACA COBIT 2019 Framework: Introduction and Methodology. 2018. Available online: https://books.google.pt/books?id=PmmDuQEACAAJ&dq=cobit+2019&hl=pt-PT&sa=X&ved=2ahUKEwjXvdGJobDvAhUMahQKHVtsC9wQ6AEwAHoECAMQAQ (accessed on 14 March 2021).
303. Strohmer, M.F.; Easton, S.; Eisenhut, M.; Epstein, E.; Kromoser, R.; Peterson, E.R.; Rizzon, E. *Disruptive Procurement: Winning in a Digital World*; Springer: Cham, Switzerland, 2020. [CrossRef]
304. Yamada, T.; Nakano, T.; Kaji, T.; Tano, S. Security Introduction Framework for Operational Technologies and Applying to Industrial Control System. In Proceedings of the 2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), Chiang Mai, Thailand, 23–26 September 2020; pp. 25–30.
305. Bizagi Process Automation: The Key to Business Continuity for Banks. 2020. Available online: https://www.bizagi.com/pt/contents/Blog/EN/process-automation-financial.html (accessed on 10 September 2022).
306. SSON Building Business Resilience with Automation. 2020. Available online: https://www.ssonetwork.com/global-business-services/articles/building-business-resilience-with-automation (accessed on 5 September 2021).
307. Mint How COVID-19 Crisis redefined IT resilience. 2021. Available online: https://www.livemint.com/industry/infotech/how-covid-19-crisis-redefined-it-resilience-11623810196852.html (accessed on 14 September 2021).
308. Berenberg, A.; Calder, B. Deployment Archetypes for Cloud Applications. *ACM Comput. Surv.* **2022**, *55*, 1–48. [CrossRef]
309. Zheng, J.; Khalid, H. The Adoption of Enterprise Resource Planning and Business Intelligence Systems in Small and Medium Enterprises: A Conceptual Framework. *Math. Probl. Eng.* **2022**, *2022*, 1–15. [CrossRef]
310. Mixson, E. Johnson & Johnson: A Crash Course in Tech-Enabled Business Resiliency | Intelligent Automation Network. 2021. Available online: https://www.intelligentautomation.network/resiliency/articles/johnson-johnson-a-crash-course-in-tech-enabled-business-resiliency (accessed on 7 November 2021).
311. Mixson, E. Digital Transformation: The Key to Unlocking Business Resilience. 2020. Available online: https://www.aidataanalytics.network/business-intelligence/articles/how-digital-transformation-unlocks-business-resilience (accessed on 27 November 2021).

312. Organizations, H.; Stronger, E. Roadmap to Recovery Helping Organizations Emerge Stronger. 2020. Available online: https://insights.crosscountry-consulting.com/roadmap-to-recovery-helping-organizations-emerge-stronger (accessed on 13 September 2021).
313. CXOToday Championing Business Continuity through Automation. 2020. Available online: https://www.cxotoday.com/corner-office/championing-business-continuity-through-automation/ (accessed on 13 September 2021).
314. Infosys Business Continuity Make Your Enterprise Resilient with the Right Partner. 2020. Available online: https://www.infosys.com/services/ai-automation/insights/documents/business-continuity.pdf (accessed on 13 September 2021).
315. Luo, Y. A general framework of digitization risks in international business. *J. Int. Bus. Stud.* **2021**, *53*, 344–361. [CrossRef]
316. Herbane, B. Rethinking organizational resilience and strategic renewal in SMEs. *Entrep. Reg. Dev.* **2018**, *31*, 476–495. [CrossRef]
317. Ardolino, M.; Bacchetti, A.; Ivanov, D. Analysis of the COVID-19 pandemic's impacts on manufacturing: A systematic literature review and future research agenda. *Oper. Manag. Res.* **2022**, *15*, 551–566. [CrossRef]
318. Carissimi, M.C.; Prataviera, L.B.; Creazza, A.; Melacini, M.; Dallari, F. Blurred lines: The timeline of supply chain resilience strategies in the grocery industry in the time of Covid-19. *Oper. Manag. Res.* **2022**, 1–19. [CrossRef]
319. Luo, Y. New connectivity in the fragmented world. *J. Int. Bus. Stud.* **2022**, *53*, 962–980. [CrossRef]
320. Services—Intelligent Automation. 2022. Available online: https://www.gooddolphin.com/intelligent-automation (accessed on 7 September 2022).
321. Consulting, N. Ensure Business Continuity with RPA. Available online: https://nuummite.com/ensure-business-continuity/ (accessed on 1 February 2022).
322. Deloitte Deloitte Global Intelligent Automation Study Reveals Acceleration in Adoption of Automation. 2020. Available online: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-intelligent-automation-study-reveals-acceleration-in-automation-adoption.html (accessed on 5 September 2021).
323. Bharti, M. Leveraging Automation for Business Continuity. 18 June 2020. Available online: https://www.uipath.com/blog/automation/business-continuity-leveraging-automation (accessed on 25 July 2021).
324. ProcessMaker Report: How Intelligent Automation Is Reshaping Business in India. 2021. Available online: https://www.processmaker.com/blog/report-how-intelligent-automation-is-reshaping-business-in-india/ (accessed on 5 September 2021).
325. Blay, K.B.; Yeomans, S.; Demian, P.; Murguia, D. The Information Resilience Framework. *J. Data Inf. Qual.* **2020**, *12*, 1–25. [CrossRef]
326. IDC Moving from Crisis to Recovery: Why Technology is Critical to Success. Mar. 2020. Available online: https://www.idc.com/ap/RESOURCES/ATTACHMENTS/5-stages-to-enterprise-recovery_enduser-ebook.pdf (accessed on 24 August 2021).
327. Tech, K. Intelligent Automation: Way Forward to Business Intelligence. 2020. Available online: https://www.kelltontech.com/kellton-tech-white-paper/intelligent-automation-way-forward-business-intelligence (accessed on 24 August 2021).
328. Development, A. Ensuring Business Continuity While Focusing on Accelerating Automation. 2020. Available online: https://www.areadevelopment.com/covid-19-response/Q2-2020/ensuring-business-continuity-focusing-accelerating-automatio.shtml (accessed on 13 September 2021).
329. Teleperformance Why RPA Is a Gamechanger in the Post-COVID-19 Era. 2020. Available online: https://www.teleperformance.com/en-us/insights-list/insightful-articles/global/why-rpa-is-a-gamechanger-in-the-post-covid-19-era/ (accessed on 8 September 2021).
330. Belhadi, A.; Mani, V.; Kamble, S.S.; Khan, S.A.R.; Verma, S. Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: An empirical investigation. *Ann. Oper. Res.* **2021**, 1–26. [CrossRef]
331. Deloitte How the Future of Work Is Transforming Our Work, Workforce, and Workplace. 2020. Available online: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-recover-dig-cap-design-digitally-enabled-flex-work.pdf (accessed on 24 August 2021).
332. roboticbiz COVID-19: RPA Is a Lifeline for Business Continuity. 2020. Available online: https://roboticsbiz.com/covid-19-rpa-is-a-lifeline-for-business-continuity/ (accessed on 5 September 2021).
333. Nintex a Business Contingency Plan with Robotic Process Automation. 2020. Available online: https://www.nintex.com/blog/your-rpa-business-contingency-plan/ (accessed on 11 October 2021).
334. Consulting, C. RPA: Providing Business Continuity during COVID-19. 2020. Available online: https://insights.crosscountry-consulting.com/rpa-providing-business-continuity-during-covid19 (accessed on 25 July 2021).
335. Cognizant Process Automation Helps Businesses Manage through Crisis. 2020. Available online: https://www.cognizant.com/perspectives/process-automation-helps-businesses-manage-through-crisis (accessed on 27 September 2021).
336. Kohli, P. Intelligent Automation Is the Key to Lasting Business Resilience. 2021. Available online: https://erp.today/intelligent-automation-is-the-key-to-lasting-business-resilience/ (accessed on 7 November 2021).
337. Dolgui, A.; Lemoine, D.; Von Cieminski, G. Advances in production management systems. In Proceedings of the Artificial Intelligence for Sustainable and Resilient Production Systems: IFIP WG 5.7 International Conference, APMS 2021, Nantes, France, 5–9 September 2021; Volume 4, p. XXVI-737. Available online: https://link.springer.com/book/10.1007/978-3-030-85910-7 (accessed on 5 September 2021).
338. Urbach, N.; Ahlemann, F.; Böhmann, T.; Drews, P.; Brenner, W.; Schaudel, F.; Schütte, R. The Impact of Digitalization on the IT Department. *Bus. Inf. Syst. Eng.* **2018**, *61*, 123–131. [CrossRef]

339. Johnston, R. Evaluating a Company's Technology: A Checklist. Value Examiner. 2020. pp. 38–41. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=141978077&site=eds-live (accessed on 5 September 2021).
340. Ravidas, S.; Karkhanis, P.; Dajsuren, Y.; Zannone, N. An Authorization Framework for Cooperative Intelligent Transport Systems. In *Emerging Technologies for Authorization and Authentication. ETAA 2019. Lecture Notes in Computer Science*; Saracino, A., Mori, P., Eds.; Springer: Cham, Switzerland, 2020; Volume 11967, pp. 16–34. [CrossRef]
341. Data, S. Top3 Misconceptions about Intellligent Automation. 2020. Available online: https://www.salixdata.com/3-common-misconceptions-about-intelligent-automation/ (accessed on 5 September 2021).
342. Kosmowski, K.T.; Piesik, E.; Piesik, J.; Śliwiński, M. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies* **2022**, *15*, 3610. [CrossRef]
343. Clark, S. Take These Critical Steps to Update Your Business Continuity Plan. 2020. Available online: https://www.reworked.co/digital-workplace/is-it-time-to-revise-your-business-continuity-plan/ (accessed on 10 September 2022).
344. ultima Business Continuity Strategy. 2021. Available online: https://www.ultima.com/business-continuity-strategy (accessed on 14 November 2021).
345. Khandate, D.V.B. Benefits and Challenges of Digital Technology. *Int. J. Sci. Res.* **2018**, 7. [CrossRef]
346. Esquivel-Vargas, H.; Caselli, M.; Laanstra, G.J.; Peter, A. Putting Attacks in Context: A Building Automation Testbed for Impact Assessment from the Victim's Perspective. In *Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2020. Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2020; pp. 44–64. [CrossRef]
347. Wolfe, J.C. *Disruption in the Boardroom: Leading Corporate Governance and Oversight into an Evolving Digital Future*; Apress: Berkeley, CA, USA, 2020. [CrossRef]
348. How to Defend Your Automation Programs from Cyber Risks. 2019. Available online: https://www.ey.com/engl/financial-services-emeia/defending-your-automation-programs-from-cyber-risks (accessed on 10 October 2021).
349. Iakovakis, G.; Xarhoulacos, C.-G.; Giovas, K.; Gritzalis, D. Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era. *Secur. Commun. Netw.* **2021**, *2021*, 1–21. [CrossRef]
350. Jackson, R.A. *Emerging Leaders*; No. October; Internal Auditor: Hong Kong, China, 2019.
351. Lim, T.; Thng, P. Outsourcing life cycle model for financial services in the fintech era. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Singapore, 7–11 March 2021; pp. 703–731.
352. Luo, Y.; Feng, J.-L. Turing Machine on Attribute Theory. In Proceedings of the 2010 IEEE International Conference on Granular Computing, San Jose, CA, USA, 14–16 August 2010; pp. 343–345. [CrossRef]
353. Crowdstrike Protect Your Robot Workforce: Extending Endpoint Protection to Robotic Process Automation (RPA) in a First-of-its-Kind Ntegration. 2021. Available online: https://www.crowdstrike.com/blog/why-extend-endpoint-protection-to-robotic-process-automation/ (accessed on 7 November 2021).
354. ITConvergence 5 Business Continuity Strategies to Help Your Planning. 2021. Available online: https://www.itconvergence.com/blog/how-to-maintain-business-continuity-5-key-strategies/ (accessed on 11 October 2021).
355. Flowable Disrupt or be Disrupted—The Need for Intelligent Process Automation. 2020. Available online: https://www.flowable.com/blog/2020/11/disrupt-or-be-disrupted-the-need-for-intelligent-business-automation/ (accessed on 8 November 2021).
356. Currey, J.; McKinstry, R.; Dadgar, A.; Gritter, M. Informed Privilege-Complexity Trade-Offs in RBAC Configuration. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, Barcelona, Spain, 10–12 June 2020. [CrossRef]
357. Kosieradzka, A.; Smagowicz, J.; Szwed, C. Ensuring the business continuity of production companies in conditions of COVID-19 pandemic in Poland—Applied measures analysis. *Int. J. Disaster Risk Reduct.* **2022**, *72*, 102863. [CrossRef] [PubMed]
358. Cyber, R. Robotic Process Automation & ML | Intelligent Mortgage Processing. 2022. Available online: https://www.royalcyber.com/resources/videos/webcasts/intelligent-mortgage-processing-with-rpa-and-ml/ (accessed on 10 September 2022).
359. Orange-Business Robotic Process Automation: Transforming Business Functions, Powering Business Resilience. Whitepaper. 2021. Available online: https://www.orange-business.com/sites/default/files/rpa_transforming-business-functions-powering-business-resilience_oct21.pdf (accessed on 24 August 2021).
360. Darmon, F. How Robotic Process Automation Helps Ensure Business Continuity in the Age of COVID-19. 2020. Available online: https://www.amdocs.com/insights/blog/how-robotic-process-automation-helps-ensure-business-continuity-age-covid-19 (accessed on 10 September 2022).

Chapter 3

Article nr. #2 – "Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019"

This article, while not the primary basis of the thesis, is an essential component, reinforcing the connection between the IEEE 2755.2:2020 standard and ISO 22301:2019. It serves as a significant contribution by providing important insights into how these standards can be mapped to better align IPA with BC. The research offers valuable input for both scholars and practitioners, emphasizing the importance of aligning automation systems with BC frameworks to enhance resilience. The article's insights into aligning IPA practices with established standards have proven instrumental in guiding the integration of automation technologies within the scope of business continuity.

It analyses the relationship between the IEEE 2755.2:2020 standard, which offers guidelines for IPA systems, and the ISO 22301:2019 standard, which outlines BCMS requirements. It developed and expanded the research during the thesis process, making it integral to its scope. The article identified key areas for further exploration, such as aligning IPA practices with BC standards to enhance resilience. It emphasized the importance of integrating automation systems with BC frameworks to streamline business processes while maintaining operational resilience. The study also highlighted the influence of automation on risk management, explored in-depth in the thesis, focusing on specific risks related to RPA within BC strategies. Furthermore, the article called attention to the need for investigations into governance and human capital dynamics within automation, which the thesis addressed by analysing how these factors are integrated within RPA strategies. Overall, this research laid the groundwork for examining the broader implications of automation technologies in governance, risk management, and compliance, ensuring alignment with business continuity frameworks.

Article Details:

- Title: "Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019."
- Date: December 4, 2023
- Journal: IEEE Access
- Scimago Journal Rank: Quartile 1 - Computer Science (all), Electrical and Electronic Engineering (all), Materials Science (all)
- Publisher: IEEE

IEEE Access
Multidisciplinary | Rapid Reviews | Open Access Journal

Received 26 October 2023, accepted 18 November 2023, date of publication 27 November 2023,
date of current version 4 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3337159

STANDARDS

Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019

JOSÉ CASCAIS BRÁS[1,2], RUBEN FILIPE PEREIRA[3], SÉRGIO MORO[4], ISAIAS SCALABRIN BIANCHI[5], AND RUI RIBEIRO[1]

[1]COPELABS, Universidade Lusófona, 1749-024 Lisboa, Portugal
[2]CGI Innovation Hub Lisbon, 1198-028 Lisboa, Portugal
[3]Instituto de Telecomunicações, Instituto Universitário de Lisboa (ISCTE-IUL), 1649-026 Lisboa, Portugal
[4]ISTAR, Instituto Universitário de Lisboa (ISCTE-IUL), 1649-026 Lisboa, Portugal
[5]Department of University Management, Federal University of Santa Catarina, Florianópolis 88040-900, Brazil

Corresponding author: José Cascais Brás (jose_manuel_bras@iscte-iul.pt)

This work was supported by COPELABS, Universidade Lusófona, Lisboa, Portugal.

ABSTRACT Organizations have been responding to possible disruptions in the organization and, at the same time, trying to increase customer satisfaction through digitising their processes. Thus, Intelligent Process Automation has been catching the latest trends in intelligent process automation due to the ease of use associated with data and requirements compliance; intelligent process automation is a step above regular automation as it mimics human behaviours and thought patterns to automate intelligently streamlines workflows and business processes. However, the constant introduction of technology via process automation in organizations can have positive and negative impacts on business continuity that need to be addressed. Although there are recent best practices, frameworks, guidelines, and standards, few studies focus on the relationship between these realms. The relationship between two sets of requirements, one for implementation practice and management methodology for intelligent software-based process automation, found in IEEE 2755.2-2020 and the other, ISO 22301-2019, about the business, to implement, maintain, and improve a management system to protect, reduce the likelihood of occurrence, prepare, respond, and recover from outages when they arise. This research is integrated into forthcoming areas for investigating the interplay between intelligent process automation and the continuity of business operations. Both are analysed and explained so that users can develop intelligent software-based process automation that complies with both frameworks in a way to embed continuity practices in an organization while optimizing business processes using Intelligent Process Automation. The study provides a bi-directional mapping for IEEE 2755.2:2020 and ISO 22301:2019, along with introducing a visual model to enhance their utility. It offers versatile applications, benefiting a wide range of stakeholders.

INDEX TERMS IEEE 2755.2:2020, ISO 22301:2019, business continuity, robotic process automation, intelligent process automation.

I. INTRODUCTION

It is unquestionable that in recent years' technological evolution has had vital effects on the operational processes of companies [1]. Recently, the COVID-19 pandemic brought this to the fore because, regardless of the organization's size, the continuous technological evolution allowed organizations to overcome this crisis with benefits that allowed companies to improve processes, train teams, offer better products to their customers, and find ways to protect organizations from

The associate editor coordinating the review of this manuscript and approving it for publication was Chih-Yu Hsu.

data breaches [2], [3]. One of the most adopted technologies was process automation which still evolving in the adoption curve [4].

Due to ever-increasing pressure to deliver value to the customer, and companies seeking to be competitive, simultaneously reducing costs and achieving efficiency gains, there has been a successive transformation in the search for alternative ways to the traditional ones to support the evaluation, planning, and decision-making of strategic decisions. From a certain point, these measures are only possible using technology, and it is at this point that the digital transformation represented by Robotic Process Automation (RPA) and Intelligent Process Automation (IPA) enters the equation [5]. This is because organizations have realized that tasks such as processing, settling, and managing transactions do not create much-added value, which due to their simplicity are potentially eligible to be automated [6], [7].

The changes related to process automation come along with proven benefits related to business efficiency, improved productivity, data security [3], [8] and effectiveness, reduced cycle time, and improved accuracy while relieving employees from repetitive and tedious tasks, but also, at the same time, contributing to a more and more complex technological environment, while still needing to ensure that their business continuity (BC) and resiliency efforts are effective [9], [10].

This brought augmented challenges to the organizations related to BC [8] and also how to find the adequate methodology of the practice for implementation and management of Software-Based Intelligent Process Automation (SBIPA).

Given the vital technology-based innovation and the progressive automation and digitization of operational, commercial, and management processes, Business Continuity Management (BCM) assumes an increased preponderance, particularly regarding the technological component. As demonstrated by the COVID-19 pandemic, which forced institutions to quickly adapt their mode of interaction with customers and employees, BCM capabilities, in operational, human, and technological aspects, are critical to avoid disruptions in the activity developed [1]. To ensure that their BC and resiliency efforts are effective in such complex environments, organizations rely on standards with IEEE/2755:2020 and ISO/22301:2019 leading [11], [12], [13].

The research question is to explore the importance of the connection between ISO 22301:2019 and IEEE 2755.2:2020 frameworks due to their relevance in the domains of BC and IPA respectively. ISO 22301:2019 is an internationally recognized standard that provides guidelines for establishing and maintaining a business continuity management system (BCMS) to ensure an organization's resilience in the face of disruptions. On the other hand, IEEE 2755.2:2020 focuses on IPA, providing a framework for organizations to leverage technologies like artificial intelligence, machine learning, and RPA to enhance their operational efficiency and decision-making capabilities.

Relating these two frameworks can bring about substantial benefits. Firstly, by integrating BC practices with IPA, organizations can strengthen their ability to respond to and recover from disruptive incidents more efficiently. IPA technologies can automate critical processes and data analysis, enabling faster decision-making during crisis situations. Secondly, incorporating BC considerations into IPA implementation ensures that automation processes are robust, secure, and capable of maintaining critical functions even during adverse events. This synergy reinforces the overall resilience of the organization's operations.

However, it's important to recognize the potential differences between these two frameworks. ISO 22301:2019 primarily focuses on risk assessment, disaster recovery, and continuity planning, while IEEE 2755.2:2020 places its emphasis on the technical aspects of implementing IPA. Understanding these distinctions lays the foundation for exploring how these standards can complement each other.

Identifying areas of convergence and divergence between ISO 22301:2019 and IEEE 2755.2:2020 is vital. This allows organizations to leverage the strengths of both standards effectively. As technology plays an increasingly vital role in business operations, aligning these two frameworks becomes pivotal for organizations aiming to enhance their resilience, maintain operational efficiency, and adapt to the ever-evolving business landscape.

In essence, investigating the relationship between ISO 22301:2019 and IEEE 2755.2:2020 is not only of academic interest but also holds practical value for organizations striving to adopt a comprehensive and forward-looking approach to BC and IPA [14].

While some best practices and standards have been proposed to guide organizations in managing these realms individually, there has been limited exploration into how they can complement and enhance each other. This research endeavors to uncover how IEEE/2755:2020 and ISO/22301:2019 can synergize, providing decision-makers with a consolidated approach that leverages understand both standards' strengths and understanding of how they can mutually support and enhance organizational resilience and IPA.

The remaining of this paper is comprised as follows. Section II presents the theoretical background. Section III describes the Method of Design Science Research (DSR). Section IV presents the design and development of the artefact. Section V presents the artefact evaluation. Finally, section VI describes the discussion and Section VII presents the conclusion and limitations of this study and future research.

II. BACKGROUND

This section defines the scope, helping to better understand the main topics of this investigation. First, an overview of the standard that supports BC activity and its evolution over time is provided. Next, the standard that supports the development of SBIPA is discussed. The last one, the section that refers

to the most used cycle in terms of quality control, is already used in the BC Standard.

A. BUSINESS CONTINUITY STANDARDS

ISO 22301:2012 was published in 2012 and replaced the British Standard for BCM BS 25999-2 [15]. It was the first internationally recognized BCM standard, and the first International Standards Organization (ISO) standard to adopt Annex L (previously Annex SL), a list of controls dedicated to management system specifications that provides a framework now common to all new management system standards published by ISO, the International Organization for Standardization.

The ISO 223XX series and its latest addendums, like all other relevant documents and other resiliency standards, are the International Organization for Standardization standards for BC and resiliency. Notwithstanding that some of these standards are applicable around the globe, many countries have their own resilience, and BC and Disaster Recovery standards, regulations, and practices [16]. Standards created by the ISO are the most widely used and have become firmly established in the U.S. Normally, ISO updates standards every 5 years. ISO 22301:2019 Security and Resilience - Business continuity management systems – Requirements [17], is the global BC standard.

Updated by ISO in 2019, this standard provides additional information to plan and execute a BCMS. It can also serve as a tool to audit business continuity programs. Table 1 summarizes the standards used to support BC.

TABLE 1. Standards to support business continuity.

Release Date	Designation	What it addresses
2003	PAS56	Business Continuity Management [18]
2005	ISO 27001 / 27002	The Information Security Standard & Information Security Management System [19]
2006	BS 25999 (1 & 2)	BSI BS25999 BS 25999 - Business Continuity [20]–[22] 1: code of practice 2: specification for BCM
2007	SI 24001:2007	Security and continuity management systems – Requirements and guidance for use of the Standards Institution of Israel (SII) [23]
2007	ISO/PAS 22399:2007	Societal security - Guideline for incident preparedness and operational continuity management [24]
2008	SS540	Singapore Standard - Singapore (SPRING) launches a new certifiable standard SS540:2008 which replaces TR 19:2004 [25].
2009	NFPA 1600	Standard on Disaster & Emergency Management and Business Continuity Programs [26].
2010	AS/NZS 5050:2010	Australian and New Zealand Business Continuity Management standard [27].
2010	ANSI/ASIS/BSI BCM.1-2010	Business Continuity Management Standard Business Continuity Management Systems: Requirements with Guidance for Use [28].
2012	ISO 223xx	Standards for BCMS Business Continuity Management [12], [15], [17], [29]–[30].
2020	NIST 800-34	Contingency Planning Guide for Information Technology Systems [31].

B. INTELLIGENT PROCESS AUTOMATION STANDARDS/FRAMEWORKS

IEEE 2755.2:2020 is a standard that provides guidelines for the development and implementation of IPA systems. The standard, titled "IEEE Standard for Intelligent Process Automation Systems - Part 2: Guidelines for the Implementation of IPA Systems," is intended to help organizations design and implement IPA systems that are efficient, effective, and secure.

The standard covers various aspects of IPA system implementation, including system architecture, data management, security, performance, and scalability. It also provides guidance on the selection and integration of different IPA technologies, such as RPA, AI, and machine learning. IEEE 2755.2:2020 is specifically designed to provide guidelines for the development and implementation of IPA systems.

IEEE 2755.2 was approved in 2020, utilising the terminology and technology taxonomy established in IEEE 2755 and IEEE 2755.1, respectively. IEEE 2755.2 provides a comprehensive self-help methodology for technology domain exploration, strategy development, technology evaluation, implementation, management, governance, operations, program optimization, and successful enterprise scaling for SBIPA programs [32], [33].

Table 2 shows some of the standards that might support the implementation of IPA. Nevertheless, IEEE 2755.2:2020 is specifically designed to provide guidelines for developing and implementing IPA systems. As such, it can be said that this standard applies to and supports the use of IPA.

C. PDCA

One of the key features of ISO 22301 is the use of the Plan-Do-Check-Act (PDCA) cycle. The PDCA cycle is a four-step management method commonly used in quality management and other fields. It is a continuous improvement approach that helps organizations to identify and address issues and continually improve their processes and systems. PDCA is also called the "Deming cycle", which is a classic quality management model promoted and practiced in Japan by W. Edwards Deming, who is considered by many to be the father of modern quality control [39]. However, he always refers to it as the "Shewhart cycle". IS0900 I: 2000 stated in its introduction that the PDCA method is available for all processes [40].

ISO 22301 uses the PDCA cycle because it is an effective way to manage BC's complex and dynamic nature. The cycle allows organizations to plan and prepare for potential disruptions, implement and test their plans, monitor and evaluate their performance, and make improvements based

TABLE 2. Standards to support process automation.

Release Date	Designation	What it addresses
2003	ISO/IEC 15504-2:2003	ISO/IEC 15504-2:2003 defines the requirements for performing process assessment as a basis for use in process improvement and capability determination [34].
2010	ISO/IEC TR 18018:2010	Information technology — Systems and software engineering — Guide for configuration management tool capabilities [35].
2015	ISO/IEC 33020:2015	This ISO/IEC standard defines a process measurement framework that supports the assessment of process capability, in accordance with the requirements of ISO/IEC 33003 [36].
2017	2755-2017	IEEE Guide for Terms and Concepts in Intelligent Process [33], [37].
2019	IEEE 2755.1-2019	IEEE Standard for Intelligent Process Automation Systems - Part 1: Framework and Concepts [38].
2020	IEEE 2755.2-2020	IEEE Standard for Intelligent Process Automation Systems - Part 2 [11].

on the results. By following the PDCA cycle, organizations can ensure that they constantly improve their BCM processes and stay prepared for future disruptions.

Järveläinen suggested that one way to incorporate good BC practices into an organization is to adopt an international standard or framework that comprehensively integrates it into existing processes [41]. The suggestion is in line with the scope of this study, which adopted ISO 22301 standards in the BC component as part of its effort to increase BCM competency and improve operational stability [22].

IEEE 2755.2:2020 [42] and ISO 22301 [17] are already robust frameworks that integrate well with other established management systems. However, they were developed as autonomous parts and, which need to be analysed to combine both in a process that can make the most of their potential.

III. RESEARCH METHODOLOGY

To pursue this research objective, the DSR methodology was chosen to build an artefact, as DSR aims to solve problems by constructing a new reality rather than explaining an existing fact or trying to help understand it.

The main elements of DSR in information systems investigations are the possibility of new research fields, the construction of new theories, or testing and validating theories. This work aims to develop a model to solve a specific problem; in this case, to understand how the IEEE and ISO standards can be combined. Therefore, DSR, widely used in information systems research to solve complex problems, may be a suitable approach for this study.

Using the DSR method was then followed for model development DSR is not only suitable for solving organizational problems in specific domains but also suitable for producing artefacts, as in the case of this model. Figure 1 presents a description of the research strategy using a DSR process and summarizes the design and development of mapping the standards under analysis.

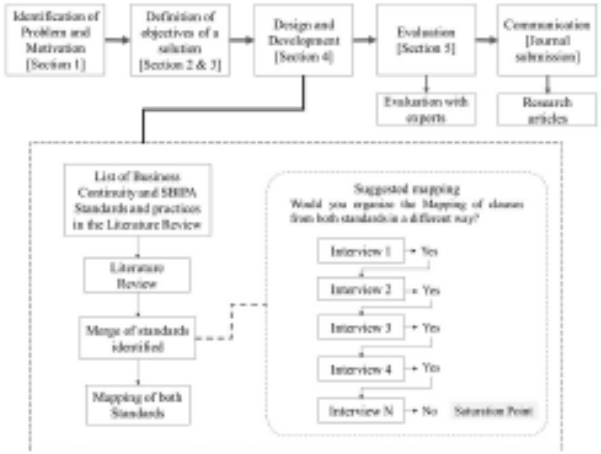


FIGURE 1. Design science research (DSR): Design and development of the mapping of both standards (adapted from [59]).

Both standards were analised to collect all data related to each clause (ISO/22301:2019) or Stage (IEEE/2755:2020).

ISO 22301:2019 applies the PDCA cycle - Plan (establish), Do (implement and operate), Check (monitor and review), and Act (maintain and improve) to implement, support, and continually improve the effectiveness of an organization's BCMS.

Following the PDCA cycle, Clauses 4 to 10 cover the following components:

- Clause 4 introduces the requirements necessary to establish the context of the BCMS applicable to the organization, as well as needs, requirements, and scope.
- Clause 5 summarizes the requirements specific to top management's role in the BCMS and how leadership articulates its expectations to the organization via a policy statement.
- Clause 6 describes the requirements for establishing strategic objectives and guiding principles for the BCMS.
- Clause 7 supports BCMS operations related to establishing competence and communication with interested parties on a recurring/as-needed basis while documenting, controlling, maintaining, and retaining required documented information.
- Clause 8 defines BC needs, determines how to address them, and develops procedures to manage the organization during a disruption.
- Clause 9 summarizes the requirements necessary to measure BC performance, BCMS conformity with this document, and to conduct a management review.
- Clause 10 identifies and acts on BCMS nonconformity and continual improvement through corrective action.

IEEE Std 2755.2–2020, IEEE Recommended Practice for Implementation and Management Methodology for Software-Based IPA, sets forth a structured methodology from inception through full adoption to establish proper programs in IPA initiatives that is broken into the following stages (later called "Clauses"):

- Stage 3 - Exploration: In this stage, stakeholders explore the organizational readiness for IPA and identify the processes that are good candidates for automation. This stage helps stakeholders understand IPA's potential benefits and risks and identify the processes that will provide the most value.
- Stage 4 - Strategy: This stage is to develop a strategy for IPA adoption, which includes defining the business case, identifying the technology solutions, and establishing a roadmap for implementation.
- Stage 5 - Evaluation: Here, stakeholders evaluate the effectiveness of the IPA solution, including the impact on business processes, employee productivity, and customer satisfaction.
- Stage 6 - Implementation: In this stage, stakeholders implement the IPA solution, which includes designing, developing, testing, and deploying the automation solution.
- Stage 7 - Management and Operations: In this stage, stakeholders manage and operate the IPA solution, which includes monitoring the solution, providing ongoing support, and ensuring that it continues to meet the organisation's needs.
- Stage 8 - Optimization and Scaling: In this stage, stakeholders optimize and scale the IPA solution, which includes identifying opportunities for improvement, implementing changes to the solution, and expanding the use of IPA across the organization.

This standard also provides an initial Clause, "General Overview.": In this stage, stakeholders provide a general overview of the IPA initiative, including the goals, scope, and desired outcomes. This stage helps establish a common understanding of the initiative across all stakeholders.

Overall, the clauses of the IEEE Recommended Practice for IPA provide a comprehensive framework for planning, implementing, and managing an IPA initiative. Each stage builds on the previous one, and all stages are designed to work together to ensure the success of the IPA initiative. This recommended practice identifies six distinct but interrelated stages in that methodology, as outlined in Clause 3 through Clause 8. These stages should be executed in sequence for an IPA initiative that is starting, but various stages are appropriate to revisit throughout the life of an IPA program.

For each stage, this standard has a structured approach including five sections (Objective, Participation, Methodology, Activities, and Outcomes) that are part of the framework for each stage of the IEEE Recommended Practice for IPA. Here is a brief explanation of each section:

- Objective: The objective section defines the goals and objectives of the stage. This section sets the direction for the activities carried out in the stage and helps stakeholders understand what they are trying to achieve.
- Participation: The participation section describes the stakeholders involved in the stage and their roles and responsibilities. This section helps ensure that all relevant stakeholders are involved in the process and understand their roles.
- Methodology: The methodology section describes the approach and methods that will be used to achieve the objectives of the stage. This section helps ensure that the activities are carried out consistently and structured.
- Activities: The activities section describes the specific tasks and activities that will be carried out in the stage. This section provides a detailed plan for implementing the methodology and helps stakeholders understand what they need to do to achieve the objectives.
- Outcomes: The outcomes section describes the expected outcomes of the stage. This section helps stakeholders understand what they are trying to achieve and provides a basis for evaluating the success of the stage.

These five sections provide a structured approach for each stage of the IEEE Recommended Practice for IPA. They help stakeholders understand what they need to achieve, how they will achieve it, and the expected outcomes. By providing a consistent framework for each stage, the IEEE Recommended Practice for IPA helps ensure that the IPA initiative is implemented in a structured and effective manner.

IV. DESIGN AND DEVELOPMENT: MAPPING PROPOSAL

This section presents the steps to develop the mapping between the two standards. The purpose of this artifact is to propose the alignment of these two frameworks, establishing connection points between the two to allow them to use their potential when implementing either of them, together or individually. The effort is to identify the points of connection between both. For this, the next section presents the integration of the clauses of the two standards based on the literature review.

In the case of IEEE 2755.2:2020, analyse to incorporate and complement the requirements of ISO 22301:2019 that relate to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving a management system to protect, reduce the probability of occurrence, prepare for, respond to, and recover from outages when they arise. Regarding ISO 22301:2019, verify the recommendations in IEEE 2755.2:2020 concerning indications to support the optimal selection, evaluation, and adoption of rapidly expanding products and services of complementary technologies available to automate corporate operational processes. Its recommendations are based on the collective knowledge and experience of developers, consultants, system integrators, service providers, and end users. A business environment is now a place of continuous technological innovation, where IPA [43] is a dynamic activity. Likewise, the underlying business

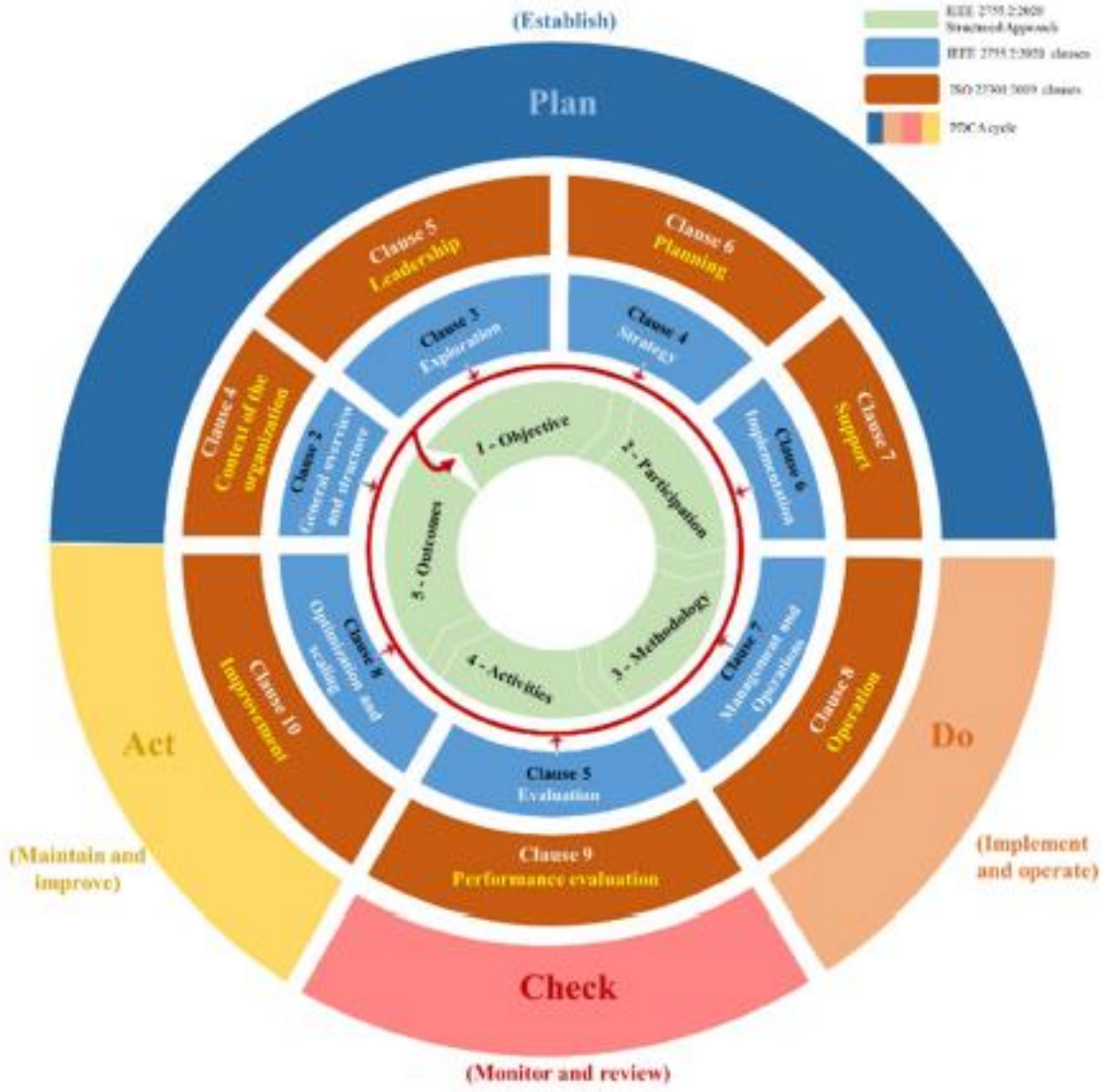


FIGURE 2. Merge of PDCA, ISO/22301:2019 and IEEE/2755:2020 clauses.

strategies and processes are constantly evolving to address new opportunities and at the same time, threats that can compromise BC, if all possibilities are not anticipated.

Both documents (IEEE 2755.2:2020 and ISO 22301:2019) have a similar word usage regarding verbs, thus, the word shall indicate mandatory requirements strictly to be followed to conform to the standard and from which no deviation is permitted (shall equals required to).

The word should indicate that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a particular course of action is preferred but not necessarily required (should equals recommended that). The word may is used to indicate a course of action permissible within the limits of the standard (may equals permitted to). The term can is used for statements of possibility and capability, whether material, physical, or causal (can equals able to).

Figure 2 represents the mapping proposal of both standards, including the already mapped PDCA cycle with ISO 22301.

Figure 2 and **Appendix A** aggregate the pre-established mapping at ISO 22301:2019 with the PDCA cycle, with the clauses for IEEE 2755.2:2020.

In the IEEE 2755.2:2020 document, each clause (stage) is fully explained with a structured approach that includes: Objective(s), Participation, Methodologies, Activities, and Outcomes, and guidance on the activities needed to complete all of the objectives of a stage comprehensively and is represented at Figure 2 with the green doughnut. Each stage succeeds the previous one and builds on the results of the last stages, establishing a logical progression of capability.

In ISO 22301:2019, Clauses 4 to 10 contain the requirements to assess compliance and can be used to determine

an organization's ability to meet its own BC needs and obligations.

A. OUTCOME OF THE MAPPINGS

The information presented in **Appendix B** correlates process outcomes required in IEEE 2755.2:2020 to process outcomes required in ISO 22301:2019. The mapping indicates related outcomes that may help meet the requirements of IEEE 2755.2:2020 when developing automation projects. There is no assumption that all the required outcomes of IEEE 2755.2:2020 are necessary to fulfil the required outcomes of ISO 22301:2019.

1) PROCESS CORRELATION

BCM is a comprehensive and holistic approach to ensuring that an organization can continue to operate during and after a disruptive event. It has the following major process to support its objectives:

i Business Impact Analysis (BIA): This process involves identifying critical business functions and the potential impacts of disruptions to those functions. It helps organizations understand their most critical processes and prioritize their BCM efforts.

ii Risk Assessment: This process involves identifying and analysing the risks that could lead to a disruptive event. It helps organizations understand the likelihood and potential impact of various risks and prioritize their risk management efforts.

iii BC Strategy Development: Based on the results of the BIA and risk assessment, organizations develop a BC strategy that outlines the steps that will be taken to ensure the continuity of critical business functions during a disruptive event.

iv Plan Development and Implementation: This process involves developing and implementing detailed plans to ensure the continuity of critical business functions during and after a disruptive event. This includes developing plans for crisis management, emergency response, and business recovery.

v Testing, Training, and Exercising: Organizations should test their plans regularly to ensure they are effective and current. Testing should include table-top exercises, simulations, and full-scale exercises. Employees should also be trained to understand their roles and responsibilities during a disruptive event.

vi Program Management: Finally, BCM is an ongoing process that requires ongoing program management. This includes monitoring the BCM program's effectiveness, making necessary changes, and ensuring that the program remains up-to-date and effective.

These processes are designed to help organizations prepare for and respond to disruptive events, minimize the impact of those events, and ensure the continuity of critical business functions.

Both IEEE Std 2755.2:2020 and ISO 22301:2019 are two different frameworks that have other objectives, however, they use a process-oriented approach for some of their major processes: knowledge acquisition, assessment, evaluation, operation, maintenance, and continuous improvement. The two, however, differ in the names of the activities of the processes.

V. EVALUATION

This section presents an assessment of the artifact. Evaluating design artifacts and design theories is a significant undertaking and a critical aspect of DSR.

To assess the proposed mapping of the clauses of ISO 22301 and IEEE 2755.2, several interviews were carried out with specialists and professionals from both areas. Interviews hold a central position in the realm of social science research, with a plethora of research method publications delving into the practice of conducting interviews in this domain [44], [45]. These interviews aim to make inferences about a population by examining a sample from that population. This contrasts with a census, which aims to make observations drawn from an entire population and are methods used for artifact evaluation. Therefore, in this study, a semi-structured questionnaire was evaluated for the proposed mapping of the clauses of ISO 22301 and IEEE 2755.2.

In this study, the artifact was evaluated in terms of construct and model with the following principles: completeness, ease of use, fidelity with real-world phenomena, internal consistency, level of detail, simplicity, Understandability, importance, accessibility, and suitability were looked at, as proposed by March and Smith [46] and Rosemann and Vessey [47]. Based on the criteria in Table 3, a semi-structured questionnaire was created.

As previously stated, assessment plays a vital and significant role in the DSR. To appraise the artifact, professionals were chosen from both the realms of BC and IPA, possessing varying levels of experience and proficiency. This decision enables us to enhance the thoroughness of the evaluation, ensuring the practical viability of the artifact. Table 3 displays the participants' area, industry, function, country, academic degree, and origin source. Table 4 shows the duration of work experience, tenure in the current position, level of responsibility, years of involvement in BC, and years of involvement in RPA/IPA.

VI. POPULATION AND SAMPLE

This study focused on integrating ISO 22301 and IEEE 2755.2 frameworks, so understanding the perspectives and experiences of experts and practitioners in the field is paramount. The population under consideration comprises professionals with expertise in BCM and IPA, from IT Business Consulting organisations, banks, and insurance companies. This includes individuals actively involved in implementing, assessing, or governance of BCM and IPA practices within their respective organizations. A purposive sampling approach will be employed to ensure comprehensive and representative insight. This will involve

TABLE 3. Semi-structured questionnaire for evaluation of the proposed clauses mapping.

	Criterion	Statement
1	Completeness	The mapping contains all the clauses of the standards of both standards.
2	Ease of use	The mapping is well-described and easy to verify and implemented in both contexts.
3	Fidelity with real-world phenomena	The proposed mapping corresponds to a possible solution to the suitable choice of practice to incorporate both standards.
4	Internal consistency	The proposed mapping uses adequate terminology, is well-written, and is justified by the theory.
5	Level of Detail	The proposed mapping contains a sufficient level of detail in each mechanism for each standard.
6	Simplicity	The proposed mapping contains the exact number of clauses for both practices and they it is easy to implement.
7	Understandability	The proposed mapping is easily understood as a model for BC and IPA and the meaning of each clause mapping is easily understandable.
8	Importance	The proposed mapping is important for both practitioners and academics.
9	Accessibility	The proposed mapping has an understandable terminology with a practice perspective, not only a theoretical one.
10	Suitability	The proposed mapping of practices is applicable in the practice to assist with BC and IPA practitioners.

identifying and selecting participants based on their demonstrable expertise and experience in ISO 22301 and IEEE 2755.2 domains. Table 5 presents the results achieved with the interviews regarding work experience, current position, responsibility, and work experience in both areas. Through semi-structured interviews, we aim to glean valuable insights that will contribute significantly to the discourse surrounding the harmonious integration of these critical frameworks.

These tables provide an overview of the characteristics of the sampled population for the study focused on integrating ISO 22301 and IEEE 2755.2 frameworks. The population consists of professionals with expertise in BCM and IPA, with select participants being extended invitations through pertinent LinkedIn reference groups [48], [49], [50], [51], [52], [53], [54], [55], [56].

Interviews are the most well-known method to collect data in qualitative research and can be used in all kinds of philosophy paradigms whether positivist, interpretive or critical [57]. The qualitative interview is an excellent way of gathering data [57]. According to Myers and Newman the interview allows collecting valuable data from people in different roles and situations [58]. Thus, interviews can be an appropriate method to develop and evaluate an artifact. Therefore, in this article, using semi-structured interviews to collect data will be used. The interviews were conducted to assess the completed artifact rather than its initial construction. The artifact under consideration was evaluated rigorously by a diverse panel of experts from various geographic, cultural, and industrial backgrounds. Notably, the interactions were limited to a single iteration, yielding no additional models or refinements as an outcome of these interviews.

Regarding the number of interviews necessary in qualitative research, Myers and Newman argues that there is a nonspecific number. It depends on the research question and what answers are being looked for. A saturation point is reached when a new insight for your research question is not found [57], [58].

In this study, we are evaluating a model with an appropriate number of clauses for BC and IPA. The proposed model is being sought, and the saturation point was reached in the fifth interview. From the fifth to twenty-two interviews, no new insights were added to the mapping model proposed.

A. WORK EXPERIENCE

A significant portion (40.9%) of the participants has over 20 years of work experience, indicating a substantial level of expertise in the field, but the same (40.9%) for the level with less expertise. No one in the range 10 – 15 years (0%), and the remaining participants fall into the categories of 5 to 10 years and 15 to 20 years, each representing 9.1% of the population.

B. CURRENT POSITION

The majority (81.8%) of the participants hold positions with 0 to 5 years of experience, indicating a relatively young workforce in their current positions. 9.1% are in positions with 5 to 10 years of experience. Only a small percentage (4.5%) are in positions with 15 to 20 years of experience, and an equal share (4.5%) have positions with over 20 years of experience.

C. RESPONSIBILITY

The responsibilities of the participants are distributed across various levels, with no particular level dominating. The highest percentage (40.9%) falls under the "Other" category, indicating diverse roles within the sampled population. This is followed by "Manager" (22.7%), "D-Level" (27.3%), and "C-Level" (9.1%).

TABLE 4. Details about the participants.

#	Area	Industry	Function	Country	Academic degree	Source
1	IT & Business Consulting	Bank	RPA Team Leader	Portugal	Bachelor	1
2	IT & Business Consulting	Insurance	RPA Developer	Portugal	Bachelor	1
3	BC	Bank	BC Analyst	Portugal	Master's degree	1
4	IT & Business Consulting	Services	VP Business Consulting	Finland	Master's degree	2
5	IT & Business Consulting	Services	Director Consulting	England	Bachelor	3
6	BC	Bank	Director Consulting	Portugal	Bachelor	1
7	IT & Business Consulting	Services	RPA Developer	Portugal	Bachelor	3
8	IT & Business Consulting	Services	VP Business Consulting	Portugal	MsC	2
9	IT & Business Consulting	Services	RPA Developer	Portugal	BsC	2
10	IT & Business Consulting	Services	RPA Developer	Portugal	Bachelor	3
11	BC and Risk	Bank	Audit Manager	Portugal	Master's degree	4
12	BC	Portuguese Road Rail Network	BC Analyst	Portugal	Bachelor	4
13	IT & Business Innovation	Insurance	Director of Organization, Innovation and Products	Portugal	Executive Master	4
14	IT & Business Consulting	Services	BC Analyst	EUA	Bachelor	1
15	IT & Business Consulting	Services	RPA Business Consultant	India	PhD	1
16	IT & Business Consulting	Services	BC Manager	Portugal	Bachelor	3
17	IT & Business Consulting for Bank & Insurance	Services	Director Consulting Services	Sweden	Master's degree	3
18	IT & Business Consulting	Services	Director Consulting	Germany	PhD Student	3
19	IT & Business Consulting	Services	Business Manager	EUA	Master's degree	1
20	IT & Business Consulting	Bank & Insurance	RPA Team Leader	Portugal	Master's degree	5
21	IT & Business Consulting	Insurance	Director Consulting	Portugal	Master's degree	3
22	IT, Business & Governance	Education	Professor	Brazil	PhD	5

Legend: [1] LinkedIn | [2] Industry Reference connection | [3] Industry Connection | [4] Client related | [5] University Link

TABLE 5. Details about the semi-structured questionnaire in the evaluation.

Rational	Indicators					
Your Work Experience	0 – 5 years	5 – 10 years	10 – 15 years	15 – 20 years	> 20 years	
	40,9%	9,1%	0%	9,1%	40,9%	
Your current position	0 – 5 years	5 – 10 years	10 – 15 years	15 – 20 years	> 20 years	
	81,8%	9,1%	0%	4,5%	4,5%	
Responsibility	C-Level	D-Level	Manager	Other		
	9,1%	27,3%	22,7%	40,9%		
Work experience in business continuity	None	1 – 5 years	5 – 10 years	10 – 15 years	15 – 20 years	> 20 years
	27,3%	45,5%	13,7%	4,5%	4,5%	4,5%
Work experience in RPA / IPA	None	1 – 5 years	5 – 10 years	> 10 years		
	22,7%	63,6%	4,5%	9,2%		

D. WORK EXPERIENCE IN BUSINESS CONTINUITY

Most participants (45.5%) have 1 to 5 years of experience in BC. 27.3% have yet to specify work experience in this area. 13.7% have 5 to 10 years of experience, while 4.5% each have 10 to 15 years and 15 to 20 years of experience.

E. WORK EXPERIENCE IN RPA/IPA

The highest percentage of participants (63.6%) have 1 to 5 years of experience in RPA/IPA, indicating a relatively high level of familiarity with this domain. 22.7% have yet to specify work experience in this area. 9.2% have more than ten years of experience in RPA/IPA, indicating a group of highly experienced individuals in this field.

In summary, the sampled population represents a diverse group of professionals with varying expertise and experience in BCM and IPA. The majority have substantial experience in their respective fields, and a significant portion also have considerable expertise in RPA/IPA. This diverse range of perspectives and experiences is expected to contribute significantly to the study's insights.

VII. DATA COLLECTION

A multi-faceted data collection approach was employed to gather comprehensive insights into integrating ISO 22301 and IEEE 2755.2 frameworks. The method involved semi-structured interviews with selected experts and practitioners. These interviews have been conducted one-on-one,

TABLE 6. Details the closed questions done to the participants and their results.

Rational	Indicators				
1. On a scale of 1 to 5, how compatible do you consider the possible combination of the "Context of the organization" clause from ISO 22301 with the "General overview and structure" clause from IEEE 2755.2?	0%	4,5%	13,6%	50%	31,8%
2. In your opinion, what level of alignment exists between the "Leadership" clause from ISO 22301 and the "Exploration" clause from IEEE 2755.2? Please rate it on a scale of 1 to 5	0%	13,6%	18,2%	59,1%	9,1%
3. Considering the combination of the "Planning" clause from ISO 22301 and the "Strategy" clause from IEEE 2755.2, how well do you perceive their synergy? Please rate it from 1 to 5	0%	0%	13,5%	50%	36,4%
4. On a scale of 1 to 5, how well do you believe the "Support" clause from ISO 22301 fits with the "Implementation" clause from IEEE 2755.2?	0%	0%	40,9%	36,4%	22,7%
5. By combining the "Management and Operations" clause from ISO 22301 and the "Operations" clause from IEEE 2755.2, how effective do you perceive this combination to be? Please rate it on a scale of 1 to 5.	0%	4,5%	18,2%	31,8%	45,5%

allowing for an in-depth exploration of their experiences, challenges, and successes in implementing these frameworks within their organizations.

Data Collection Process: The interview process started by requesting consent and an introduction to the study's objectives. Closed questions with a rating scale of 1 to 5 (1 being the lowest, five being the highest) with optional comments to each question have been used to encourage participants to share their perspectives freely regarding the combination of each clause. Their results are expressed in Table 6. The analysis involved a systematic review to extract key information on how well each clause combines or fits together relating BCM and IPA. An additional question was posed for the participants to share any insights, concerns, or potential advantages they might foresee in implementing this integrated approach.

Data Interpretation: The collected data aimed at identifying recurring patterns, themes, and significant points raised by the participants. Through this process, commonalities and differences in perspectives have been identified, providing valuable insights into the challenges, successes, and potential synergies between ISO 22301 and IEEE 2755.2, involving triangulating the findings from both interview transcripts and proposal analysis, ensuring a comprehensive understanding of the integration landscape.

VIII. RESULTS AND DISCUSSION

This section discusses the results of the optional comment requested for each question. **Appendix C** presents all the information related to the comments made by the participants for each question presented (Q1 to Q8).

Q1. "Context of the organization" clause from ISO 22301 with the "General overview and structure"

Respondents generally perceive a high level of compatibility between the "Context of the organization" clause from ISO 22301 and the "General overview and structure" clause from IEEE 2755.2. The majority (81%) rated the combination as a 4 or 5, indicating a solid alignment.

As seen in **Appendix C - Q1**, the feedback emphasizes that aligning the organizational context with the general structure provides a solid foundation for BCM and IPA initiatives.

This understanding is crucial for effective planning and automation efforts. The combination supports risk mitigation by allowing for a nuanced assessment of potential risks and vulnerabilities based on the organizational context.

This enables more targeted and effective selection and implementation of automation solutions to enhance BC. The integration of these clauses aids in optimizing resource allocation for automation projects. It ensures that automation efforts are directed towards functions and processes foremost vital to the organization's overall structure and objectives. The integration establishes a foundation for the long-term alignment of automation efforts with organizational goals.

This ensures that automation strategies evolve in sync with organizational structure and objectives changes, providing sustained support for BC initiatives. Combining these clauses leads to a comprehensive understanding of the organizational landscape, enabling a more informed and strategic approach to BC and automation initiatives. This alignment ensures that automation efforts are closely aligned with the overall structure and objectives of the organization.

Overall, the responses suggest a strong consensus among the respondents regarding the compatibility and adequacy of combining these clauses. The alignment between the organizational context and the general structure is critical in facilitating effective planning and automation efforts for BCM and IPA initiatives.

Q2. "Leadership" clause from ISO 22301 and the "Exploration" clause from IEEE 2755.2

Respondents broadly recognize a substantial degree of alignment between the "Leadership" clause from ISO 22301 and the "Exploration" clause from IEEE 2755.2. The majority (68.2%) rated the alignment as either a 4 or 5, indicating a strong perceived alignment.

Some respondents expressed a degree of uncertainty or suggested that, based solely on the wording and context, they did not see an immediate fit between the clauses. This indicates that a deeper understanding of the specific clauses may be needed to appreciate the alignment. There is a viewpoint that the "Exploration" clause is a vast subset of what ISO 22301 describes. However, it's noted that if the intent is to use ISO as a tie-breaker between implied frameworks, this alignment could be appropriate. It suggests that there may be a hierarchical relationship where one standard complements or supplements the other. Feedback emphasizes that effective leadership, as outlined in ISO 22301, is pivotal

in driving informed decisions regarding IPA initiatives. The "Exploration" clause complements this by emphasizing the need for comprehensive documentation, including motivations, dependencies, and competitive analysis. This ensures that leadership is well-informed and equipped to drive IPA initiatives forward. The combination of "Leadership" and "Exploration" is seen as providing a solid foundation for turning strategic vision into actionable plans. This alignment ensures that the vision is supported by a detailed roadmap, incorporating documentation of motivations, dependencies, and competitive analysis. The feedback highlights the pivotal role of leadership in driving the adoption of automation technologies. A forward-thinking approach to exploration can uncover opportunities for utilizing automation to enhance BCM strategies, allowing organizations to respond more effectively to unforeseen events. It's suggested that there may also be a match between the "Leadership" clause and Clause #7 ("Management & Operations"). This indicates recognition of potential interrelationships between multiple clauses.

Overall, as presented in **Appendix C - Q2**, the responses indicate a perceived strong alignment between the "Leadership" clause from ISO 22301 and the "Exploration" clause from IEEE 2755.2. This alignment is seen as providing a solid foundation for driving informed decisions and exploring opportunities for automation within the context of BC.

Q3. "Planning" clause from ISO 22301 and the "Strategy" clause from IEEE 2755.2

Respondents generally acknowledge a high level of synergy between the "Planning" clause from ISO 22301 and the "Strategy" clause from IEEE 2755.2. The majority (86.4%) rated the synergy as either a 4 or 5, indicating a strong perceived alignment.

The feedback emphasizes that both clauses focus on actions to address risks and opportunities. "Planning" within the BCMS context emphasizes risk assessment and mitigation, while "Strategy" in the IPA context involves controlling deployment risks managing. This alignment ensures that risk management is integrated into BCMS planning and IPA strategy development. "Planning" and "Strategy" are fundamentally aligned in their focus on strategic thinking. "Planning" encompasses the development of a structured approach to BC, while "Strategy" guides formulating a broader organizational strategy that may include automation initiatives. This alignment ensures that planning efforts are integrated into the larger strategic framework. Measurable objectives are highlighted as crucial for both BCMS and IPA initiatives. The "Planning" clause's emphasis on measurable objectives aligns with the "Strategy" clause's aim to assess how IPA can support and enhance the enterprise's strategic plan. This alignment ensures progress can be effectively tracked, monitored, and communicated in line with the sustainability concept. Automation is viewed as a significant augmentation to the effectiveness of BCM plans, contributing to both efficiency and environmental sustainability. It can streamline processes related to continuity planning, enabling faster response times and reducing human error in critical scenarios. This suggests that integrating automation into the planning process enhances the overall effectiveness of BCM while aligning with the sustainability concept. The integration ensures that automation efforts are not viewed in isolation but are considered an integral part of the overall BC strategy. This emphasizes that automation is a strategic component of BC planning, emphasizing its role within the sustainability concept rather than as a separate initiative.

Overall, as shown in **Appendix C - Q3**, the responses indicate a perceived strong synergy between the "Planning" clause from ISO 22301 and the "Strategy" clause from IEEE 2755.2. This alignment is seen as providing a solid foundation for integrating automation into the broader BC planning process, ultimately enhancing the effectiveness of BCM plans.

Q4."Support" clause from ISO 22301 with the "Implementation" clause from IEEE 2755.2

Respondents generally perceive a high level of compatibility between the "Support" clause from ISO 22301 and the "Implementation" clause from IEEE 2755.2. The majority (59.1%) rated the fit as either a 4 or 5, indicating a strong perceived alignment.

The feedback emphasizes that support is crucial during the implementation stage. With adequate support, the success of the implementation may be better. This highlights the importance of having resources and expertise available to ensure a smooth implementation process. Both clauses are seen as complementing each other. The "Support" clause addresses potential challenges, such as skill gaps or resource constraints, which can be critical to the success of the implementation. This synergistic approach increases the likelihood of a successful automation deployment. Integrating "Support" from ISO 22301 with "Implementation" from IEEE 2755.2 is viewed as leading to enhanced operational efficiency. Adequate support regarding skilled personnel, technology infrastructure, and training ensures that automation initiatives directly contribute to the resilience of critical business functions. The combination of "Support" and "Implementation" underscores the critical need for resource allocation and training. "Support" ensures that the right resources, including personnel and technology, are allocated for the successful "Implementation" of automation solutions. This alignment is seen as vital for achieving BC and efficiency goals.

Overall, as illustrated in **Appendix C - Q4**, the responses suggest a strong consensus among the respondents regarding the compatibility and adequacy of combining the "Support" clause from ISO 22301 with the "Implementation" clause from IEEE 2755.2. This alignment is essential for ensuring a smooth and successful implementation of automation technologies within the context of BC.

Q5." Management and Operations" clause from ISO 22301 and the "Operations" clause from IEEE 2755.2

Respondents generally perceive a high level of effectiveness in combining the "Management and Operations"

TABLE 7. Relationship between the PDCA Cycle, clauses of ISO 22301:2019 and IEEE 2755.2:2020 addressing PDCA component.

PDCA component	ISO 22301:2019	IEEE 2755.2:2020
Plan (Establish)	**Clause 4** ("Context of the organization") **sets out** what the organization **should do** to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including: — the needs and expectations of interested parties; — its legal and regulatory obligations; — the required scope of the BCMS.	**Clause 2** ("General overview and structure") The objective is to **investigate** the suitability of an IPA initiative for a business unit or business before **setting out** any strategic directives. The investigation is completed by leveraging a variety of people, tools, and methodologies along with defined industry practices to understand the relevant pros and cons of IPA adoption.
	Clause 5 ("Leadership") **sets out** management's role in demonstrating commitment, defining policy, and establishing roles, responsibilities and authorities.	**Clause 3** ("Exploration") The objective is to **investigate** the suitability of an IPA initiative for a business unit or business before **setting out** any strategic directives. The investigation is completed by leveraging a variety of people, tools, and methodologies along with defined industry practices to understand the relevant pros and cons to IPA adoption
	Clause 6 ("Planning") describes the actions for **establishing strategic** objectives and guiding principles for implementing the BCMS.	**Clause 4** ("Strategy") Based on the findings and insights gained from the Exploration stage, the Strategy stage aims to **assess** how IPA can support and enhance the enterprise strategic business plan and technology environment in ways that maximize opportunities and benefits while controlling risks.
	Clause 7 ("Support") **identifies** the BCMS elements that should be in place, namely resources, competence, awareness, communication and documented information.	**Clause 6** ("Implementation") The purpose is to **design, configure, build, test,** and **deploy** automation that will deliver the targeted business outcomes identified in the Strategy stage using the architectures and technologies selected for deployment in the Evaluation stage.
Do (Implement and operate)	**Clause 8** ("Operation") identifies the processes for **establishing** and maintaining BC.	**Clause 7** ("Management and operations") The objectives are to assure the reliable performance of automations in production and to **identify new** deployment opportunities for current automation tools and new IPA tools that can enhance capability, performance, and value.
Check (Monitor and review)	**Clause 9** ("Performance evaluation") **provides the basis** for improving the BCMS through measurement and evaluation its performance.	**Clause 5** ("Evaluation") The objective is to **select** the most appropriate technologies and product architectures to deliver the outcomes and benefits identified in the Strategy workstream. NOTE—IEEE Std 2755.1–2019 provides a comprehensive technology evaluation guide
Act (Maintain and improve)	**Clause 10** ("Improvement") covers the corrective action for **addressing** nonconformity identified through performance evaluation.	**Clause 8** ("Optimization and scaling") Aims to **support** the sustainable growth of IPA programs while mitigating risks. When scaled, IPA technologies create additional value by improving productivity, expanding enterprise capacity, and supporting the expansion of new products, solutions, and business models.

clause from ISO 22301 and the "Operations" clause from IEEE 2755.2. The majority (77.3%) rated the combination as either a 4 or 5, indicating a strong perceived alignment.

The feedback emphasizes that operation and management are closely intertwined. Even though operations may have a routine nature, effective leadership is crucial. This highlights the importance of vigilant oversight and collaboration between operations and management. The need for continuous assessment of BCM and IPA performance metrics is recognised. Automation processes are considered integral to the overall assessment of BC effectiveness, indicating that automation can enhance the measurement and evaluation of BCM initiatives. Both clauses are viewed as emphasizing the importance of operational planning and control. "Management and Operations" focuses on planning and controlling BCM support processes, while "Operations" in the context of IPA aims to sustain and expand automation programs. This alignment ensures that operational processes are well-planned and effectively executed in BCM and IPA initiatives. Combining "Operation" and "Management and Operations" is seen as seamlessly integrating automation processes into day-to-day operations. This optimization of routine tasks enhances the organization's overall resilience by ensuring that critical processes are consistently maintained. Both clauses are seen as highlighting the preparation of plans and procedures. In BCM, this ensures readiness to respond to disruptions. In the context of IPA, it supports the sustainable growth of automation programs. This alignment underscores the importance of well-defined plans and procedures in both initiatives. The alignment between the two clauses is emphasized as supporting risk mitigation in both BCM operations and IPA initiatives. This highlights the critical role of risk management in operational activities for both BCM and IPA. The combination is described as a perfect match, indicating a strong compatibility and complementarity between the "Management and Operations" clause and the "Operations" clauses.

Overall, as displayed in **Appendix C - Q5**, the responses suggest a strong consensus among the respondents regarding the effectiveness of combining these clauses. Integrating management and operations with operational processes is seen as a powerful approach to enhancing the organization's resilience and effectiveness in both BCM and IPA initiatives.

TABLE 8. PDCA, ISO 22301:2019 & IEEE 2755.2:2020 outcomes.

PDCA compoment	ISO 22301:2019	Outcomes	IEEE 2755.2:2020	Outcomes
Plan (Establish)	**Clause 4** ("context of the organization")	- Determine external and internal issues that are relevant to his purpose and affect your ability to achieve their BCMS results(s); - which stakeholders and requirements are relevant to BCMS; - Legal and regulatory requirements (for this must have a process to have the ability to identify, access, and evaluate the continuity of their products and services, activities, and resources); - Scope of Business Continuity Management Systems (Internal and External Issues; Requirements, Mission, Objectives, and Internal and External Obligations); - Implement a BCMS	**Clause 2** ("General overview and structure")	- Overall, the outcomes are intended to provide stakeholders with a clear understanding of the standard', as well as the key concepts and definitions used throughout the document. This sets the foundation for applying the standard to an IPA initiative and helps ensure that all stakeholders are on the same page
	Clause 5 ("leadership")	- High Management must demonstrate leadership and commitment by ensuring that the policy of continuing the predefined business is communicated, as well as who are the interveners and their responsibilities and which objectives are established, providing all the necessary resources and promoting continuous improvement.	**Clause 3** ("Exploration")	- Documented and clearly defined business-focused vision; - Documented identification and categorization of the instant motivations for exploring the potential of an IPA initiative; - Documented identification of dependencies of an IPA initiative or factors that conflict; - Documented competitive analysis to understand existing supplier; - Documented review with conclusions and considerations collected through the Exploration stage that support the recommendation to proceed or not.
	Clause 6 ("planning")	By planning BCMS to determine which objectives to be achieved, the actions to face risks and opportunities to ensure that BCMS achieves the intended results, preventing or reducing unwanted effects and achieving continuous improvement. These should be measurable, monitored, communicated, and tied as appropriate, incorporating change management techniques whenever necessary.	**Clause 4** ("Strategy")	- Maybe a new or significantly revised enterprise strategic plan, including prospective outcomes, benefits, and risks associated with deploying IPA, along with a high-level timetable and operating budget for the IPA initiative
	Clause 7 ("support")	The organization must determine and provide all the necessary resources to establish, implement, maintain and improve the BCMS. These resources must have the necessary skills and capabilities and be aware of the policies in force and the implications for not being in accordance. The organization must determine internal and external communications relevant to BCMs, creating and maintaining records in a controlled manner and allowing their distribution only to those who are authorized.	**Clause 6** ("Implementation")	- The deliverables from the implementation stage of work consist of fully tested and validated automation, including software, complete documentation, instructional materials, policies, procedures, and performance monitoring methods—all information, training, and practice guides required for controllers to run the automated processes safely and reliably at enterprise scale during the Management and Operations stage of work.

Q6. "Evaluation" clause from ISO 22301 and the "Performance Evaluation" clause from IEEE 2755.2

Respondents overwhelmingly perceive a high level of compatibility between the "Evaluation" clause from ISO 22301 and the "Performance evaluation" clause from IEEE 2755.2. The majority (95%) rated the compatibility as either a 4 or 5, indicating a strong perceived alignment.

There's a view that "Evaluation" and "Performance evaluation" look similar. Unless the word "performance" refers explicitly to evaluating the performance of the evaluation process itself, the objectives appear to be expected. This suggests a natural overlap in their focus on measurement and assessment. The adequacy of the integration is seen as 100%, indicating a high level of confidence in the compatibility and effectiveness of combining these clauses. Both clauses are seen as highlighting the need for measurement and assessment. "Evaluation" in ISO 22301 focuses on BCMS performance, while "Performance evaluation" in IEEE 2755.2 addresses the review of IPA programs. This alignment ensures that performance is systematically measured in both BCM and IPA initiatives to support growth while mitigating associated risks. While the integrated approach holds tremendous promise, there may be challenges in harmonizing certain aspects of BCM with automation. This includes ensuring that automated processes align with BC objectives without compromising security, which requires careful consideration. The integration is seen as an opportunity for improvement in both BCM and automation. It can lead to optimizing and scaling automation processes, ultimately resulting in more resilient and efficient BC strategies. Integrating "Performance Evaluation" and "Evaluation" is viewed as making performance evaluation more comprehensive. Automation of performance metrics allows for real-time monitoring of key indicators, enabling proactive adjustments

TABLE 8. *(Continued.)* ISO 22301:2019 & IEEE 2755.2:2020 outcomes.

PDCA component	ISO 22301:2019	Outcomes	IEEE 2755.2:2020	Outcomes
Do (Implement and operate)	**Clause 8** ("operation")	The organization must operationally plan and control BCM support processes to meet all requirements, implementing the processes and actions required to meet all criteria. It should perform business impact analysis and risk assessment over time, determining its order, and the types and impact criteria relevant to the context of the organization, to identify and elaborate BC strategies and solutions. The risk assessment process is addressed in ISO 31000. Other outcomes are preparing the BC's plan and procedures and allocating resources to implement the solutions and strategies to the risks raised, allowing you to alert and communicate effectively.	**Clause 7** ("Management and Operations")	- Cost/benefit analysis of automation in production—including hours returned to the business, improvement in quality or audit performance, enhanced throughput, and others—guides where further optimization or scale potential is possible.
Check (Monitor and review)	**Clause 9** ("performance evaluation")	An organization will be able to evaluate the performance and effectiveness of its BCMS and verify if it ensures that its intended outcomes are achieved by auditing: • whether the BCMS meets the needs of the organization • conforms to the requirement of ISO 22301:2019 • how consistently processes and procedures are being applied • whether processes and procedures achieve the intended results.	**Clause 5** ("Evaluation")	- Specific measurements [in the form of critical success factors (CSFs)] and deliverables that should be documented for evaluation, decision-making, and post-decision planning for the Implementation stage of work (Demonstration with key attributes and requirements, Proof of concept and pilot). The deliverables from the PoC stage should be a working automation.
Act (Maintain and improve)	**Clause 10** ("improvement")	The main purpose for implementing a BCMS is to ensure an organization can respond to a disruptive incident promptly on time, and to continue delivering its key products and services at a pre-defined level until return to normal operations can be affected. For this, need to determine opportunities for improvement and implement actions to achieve its intended outcomes of its BCMS, react to nonconformities, take action to control and correct the non-conformities, deal with the consequences, find the root cause, and investigate nonconformities. Any corrective actions identified to address nonconformities will be implemented without delay. The corrective action implemented is to be reviewed to determine its effectiveness.	**Clause 8** ("Optimization and Scaling")	- Measurements and deliverables in the optimizing and scaling stage include a set of metrics, KPIs, decisions, and action items that contribute to the program's overall growth and value generation. Programs should tailor the metrics and KPIs to meet their needs, and then use them to drive decisions and activities required to continue to optimize and scale the program.

to both automation processes and BCM strategies as needed.

Overall, as exposed in **Appendix C - Q6**, the responses suggest a strong consensus among the respondents regarding the compatibility and adequacy of combining the "Evaluation" clause from ISO 22301 with the "Performance evaluation" clause from IEEE 2755.2. This alignment is viewed as crucial for systematically measuring and assessing performance in both BCM and IPA initiatives, supporting growth while mitigating associated risks.

Q7. "Optimization and scaling" clause from ISO 22301 and the "Improvement" clause from IEEE 2755.2

Respondents overwhelmingly perceive a high level of compatibility between the "Optimization and scaling" clause from ISO 22301 and the "Improvement" clause from IEEE 2755.2. The majority (86.4%) rated the compatibility as either a 4 or 5, indicating a strong perceived alignment.

There's a view that while "Improvement" is a broader concept than "optimization and scaling," their objectives are fully compatible. This suggests a natural overlap in their focus on driving enhancements and expansions in processes and initiatives. The integration is seen as key to efficient resource utilization for automation projects. It ensures that resources are allocated in a way that enhances current processes and allows for scaling automation initiatives. This targeted approach maximizes the impact of automation on BC. It is emphasized that the integration of 'Optimization and scaling' with 'Improvement' is crucial for maximizing the return on investments in automation. Improvements are seen as contributing not only to the current state but also to the scalability and optimization of automation solutions, enhancing their overall value in BC. Respondents specifically highlight that both clauses are compatible, indicating a strong consensus on their alignment. The combination is

TABLE 9. Summary of the main comments regarding questions 1 to 3 (these comments were optional to the closed questions).

Question	Comments
Q1.	"Alignment enables standardization, which enables easier awareness and understanding"
	"In my opinion, as a whole, the identified clauses make a very solid and pertinent match. However, and in a paradigmatic way, clause 7 (Management and Operations) presents a very strong and unequivocal connection."
	"I highlight that aligning the organizational context with the general structure provides a solid foundation for BCM and IPA initiatives. Both permit the understanding of the organization's structure that is crucial for effective planning and automation."
	"The 'Context of the Organization' clause emphasizes the importance of understanding the internal and external factors that influence an organization. Combined with the 'General overview and structure,' it ensures that automation is integrated seamlessly within the existing organizational framework. This alignment is crucial for achieving continuity objectives while leveraging automation technologies."
	"This integration can support risk mitigation, as by understanding the organizational context allows for a more nuanced assessment of potential risks and vulnerabilities. This contextual awareness guides the selection and implementation of automation solutions in a way that enhances business continuity efforts.
	"The integration of 'Context of the Organization' and 'General overview and structure' aids in optimizing resource allocation for automation projects. It ensures that automation efforts are prioritized and directed towards functions and processes foremost vital to the organization's overall structure and objectives. This targeted approach maximizes the impact of automation on business continuity."
	"It can establish a foundation for long-term alignment of automation efforts with organizational goals. This ensures that automation strategies evolve in sync with organizational structure and objectives changes, providing sustained support for business continuity initiatives."
	If we integrate 'Context of the Organization' with 'General overview and structure,' we establish a comprehensive understanding of the organizational landscape. This enables a more informed and strategic approach to both business continuity and automation initiatives. The 'Context' clause ensures that automation efforts are aligned with the overall structure and objectives of the organization."
Q2.	"Have doubts about the relation between Leadership (ISO) and Exploration (IEEE)"
	"The 'Leadership' clause, emphasizing clear communication of predefined business policies and objectives, aligns seamlessly with the 'Exploration' focus on a documented and business-focused vision. When high management effectively communicates the strategic vision, it provides a foundation for the detailed exploration of an IPA initiative's potential motivations and dependencies."
	"Not knowing in detail the clauses, looking only at the words and the context of them, it doesn't seem to have a fit."
	"It's an appropriate mapping, but as a mapping, the exploration clause is a vast subset of what 22301 describes. If the intent, though, is that by this mapping that, ISO is the tie-breaker between what is the implied framework of each (each inherits the strengths and weaknesses of the other, as a result), then ok, but otherwise (if no implied inheritance), it should be noted as separated."
	"Both can emphasize the importance of leadership in driving BCM and IPA efforts and how an exploratory approach to automation can uncover opportunities for improving business continuity strategies."
	"Effective leadership, as outlined in ISO 22301, empowers high management to make informed decisions regarding IPA initiatives. The 'Exploration' clause complements this by emphasizing the need for comprehensive documentation, including motivations, dependencies, and competitive analysis. This ensures that leadership has the necessary insights to drive the initiative forward."
	"The 'Leadership' clause, emphasizing the communication of predefined business policies and objectives, provides the foundation for turning the strategic vision into actionable plans. This aligns with the 'Exploration' clause's focus on documenting motivations, dependencies, and competitive analysis, ensuring that a detailed roadmap supports the vision."
	"Highlights the pivotal role of leadership in driving the adoption of automation technologies. A forward-thinking approach to exploration can uncover opportunities for utilizing automation to enhance BCM strategies, allowing organizations to respond more effectively to unforeseen events."
	"Leadership's role in providing resources aligns with the 'Exploration' clause's focus on identifying dependencies and conflicts. This combination might ensure that leadership is equipped to proactively manage risks and resolve conflicts that may arise while exploring an IPA initiative."
	"It should be considered to find also a match between Clause #7 (Management & Operations)."
Q3.	"Planning must follow a strategy direction and definition, so I believe they have high compatibility."
	"Clauses match Perfectly."
	"Both 'Planning' and 'Strategy' clauses emphasize actions to face risks and opportunities. 'Planning' within the BCMS context focuses on risk assessment and mitigation, while 'Strategy' in the IPA context involves controlling deployment risks. This alignment ensures that risk management is integral to BCMS planning and IPA strategy development."
	"From my point of view, the 'Planning' clause from ISO 22301 and the 'Strategy' clause from IEEE 2755.2 are fundamentally aligned in their focus on strategic thinking. 'Planning' encompasses the development of a structured approach to business continuity, while 'Strategy' guides formulating a broader organizational strategy that may include automation initiatives. This alignment ensures that planning efforts are integrated into the larger strategic framework."
	"The match that was perceived is completely accurate and needed."
	"The 'Planning' clause emphasizes that objectives should be measurable and tied appropriately. This aligns with the 'Strategy' clause, which aims to assess how IPA can support and enhance the enterprise's strategic plan. Measurable objectives are crucial for BCMS and IPA initiatives, ensuring that progress can be tracked, monitored, and communicated effectively."
	"A well-supported automation strategy can significantly augment the effectiveness of BCM plans. Automation can streamline processes related to continuity planning, enabling faster response times and reducing human error in critical scenarios.
	"The 'Planning' clause emphasizes the need for structured business continuity plans. When integrated with the 'Strategy' clause, it ensures that automation initiatives are included as a strategic component of these plans. This alignment ensures that automation efforts are not viewed in isolation but are integral to the overall business continuity strategy."
	"Improvement in BCM and automation can go hand-in-hand to optimizing and scaling automation processes and lead to more resilient and efficient business continuity strategies."
	"Evaluating performance becomes more comprehensive with the integration of 'Performance Evaluation' and 'Evaluation', as the automation of performance metrics allows for real-time monitoring of key indicators, enabling proactive adjustments to both automation processes and BCM strategies as needed."

viewed as a way to future-proof automation initiatives. This integration ensures that automation solutions are effective today and designed to adapt and grow with the organization. It provides a strategic advantage in maintaining BC in a constantly evolving business landscape. The combination establishes a framework for iterative enhancement. It ensures

TABLE 9. *(Continued.)* **Summary of the main comments regarding questions 4 to 6 (these comments were optional to the closed questions).**

Question	Comments
Q4.	"During an implementation stage, support must be included or at least it must follow the implementation; without support the success of the implementation is questionable, to say the least."
	"Both complement each other."
	"It can mitigate the risks associated with implementing automation technologies. The 'Support' clause from ISO 22301 ensures that potential challenges such as skill gaps or resource constraints are addressed proactively, minimizing the likelihood of implementation setbacks. This synergistic approach increases the likelihood of successful automation deployment."
	"The integration of 'Support' from ISO 22301 with 'Implementation' from IEEE 2755.2 can lead to enhanced operational efficiency. The 'Support' clause emphasizes the importance of resources and competence, directly contributing to the effective 'Implementation' of automation processes. Adequate support ensures that the implementation is seamless and optimized for maximum impact."
	"The 'Support' clause from ISO 22301 complements the 'Implementation' clause from IEEE 2755.2 by ensuring that the implementation of automation technologies aligns seamlessly with the organization's business continuity goals. Adequate support regarding skilled personnel, technology infrastructure, and training ensures that automation initiatives contribute directly to the resilience of critical business functions."
	"The integration of 'Support' and 'Implementation' highlights the critical need for resource allocation and training. 'Support' ensures that the right resources, including personnel and technology, are allocated for successful 'Implementation' of automation solutions. This can help in achieving the intended business continuity and efficiency goals."
Q5.	"Operation and management go hand-by-hand, even though the perceived routine nature of operations, management must be watchful and work closely."
	"See my comments from #2 above."
	"There is a need for continuous assessment of BCM and IPA performance metrics. Therefore, automation processes can be integrated into the overall assessment of business continuity effectiveness."
	"Both 'Management and Operations' and 'Operations' clauses emphasize the importance of operational planning and control. 'Management and Operations' focuses on planning and controlling BCM support processes, while 'Operations' in the context of IPA aims to sustain and expand automation programs. This alignment ensures that operational processes are well-planned and effectively executed in BCM and IPA initiatives."
	"Direct connection"
	"From my point of view ', Management and Operations' and 'Operations' clauses highlight the preparation of plans and procedures. In BCM, this ensures readiness to respond to disruptions. In the context of IPA, it supports the sustainable growth of automation programs. This alignment underscores the importance of well-defined plans and procedures in both initiatives."
	"The combination of 'Operation' and 'Management and Operations' ensures that automation processes are seamlessly integrated into day-to-day operations. This also optimises routine tasks and enhances the organization's overall resilience by ensuring that critical processes are consistently maintained."
	"The 'Management and Operations' clause in ISO 22301 emphasizes mitigating risks in BCM operations. This aligns with the objective of the 'Operations' clause in IEEE 2755.2, which seeks to mitigate risks while expanding enterprise capacity through IPA. Both clauses highlight the importance of risk management in operational activities."
	"Nevertheless, we find a perfect match on this; we are upon a strong compatibility and complement related."
Q6.	"Again, not knowing the details of the clauses evaluation and performance evaluation look similar and unless the word performance if specific of looking at how the 'performance' of the evaluation itself I would say the objectives are common."
	"Adequacy is 100%"
	"Having the wide scope related with the 'Evaluation' concept, we cover all the key areas related, namely auditing, risk impacts, reporting, ... So, the 'marriage' between both is very natural and strong."
	"Both 'Evaluation' and 'Performance evaluation' clauses highlight the need for measurement and assessment. 'Evaluation' in ISO 22301 focuses on BCMS performance, while 'Performance evaluation' in IEEE 2755.2 addresses the assessment of IPA programs. This alignment ensures that performance is systematically measured in both BCM and IPA initiatives to support growth while mitigating associated risks."
	"While this integrated approach holds tremendous promise, there may be challenges in harmonizing certain aspects of BCM with automation. For instance, ensuring that automated processes align with business continuity objectives without compromising security is a critical concern that requires careful consideration."
	"Improvement in BCM and automation can go hand-in-hand to optimizing and scaling automation processes and lead to more resilient and efficient business continuity strategies."
	"Evaluating performance becomes more comprehensive with the integration of 'Performance Evaluation' and 'Evaluation', as the automation of performance metrics allows for real-time monitoring of key indicators, enabling proactive adjustments to both automation processes and BCM strategies as needed."

that automation solutions are also optimized for current operations and scalable to accommodate future needs. This promotes a culture of continuous improvement, driving sustained benefits for BC.

Overall, as exhibited in **Appendix C - Q7**, there is a recognition of the significant potential in reshaping the intersection of BCM and IPA through integrating clauses from ISO 22301 and IEEE 2755.2. This integrated approach is seen as revolutionizing how organizations approach BC and automation, leading to a more resilient and efficient operational model. However, it's noted that robust change management processes, stakeholder buy-in, and training are crucial for successful implementation and maximizing the benefits of this integrated approach.

Q8. "In your expert opinion, considering the integration of clauses from ISO 22301 and IEEE 2755.2, how do you envision this combined framework influencing the intersection of Business Continuity Management (BCM) and Intelligent Process Automation (IPA)? Please share any insights, concerns, or potential advantages you foresee in implementing this integrated approach".

Based on the feedback provided, as demonstrated in **Appendix C - Q8**, there is a strong consensus among participants that integrating ISO 22301 and IEEE 2755.2 holds

TABLE 9. *(Continued.)* Summary of the main comments regarding questions 7 to 8 (these comments were optional to the closed questions).

Question	Comments
Q7.	"Improvement is again a concept larger than "optimization and scaling" but forgetting the specifics of the wordings I say they are fully compatible."
	"Integrating 'Optimization and scaling' with 'Improvement' leads to efficient resource utilization for automation projects. It ensures that resources are allocated in a way that enhances current processes and allows for scaling automation initiatives. This targeted approach maximizes the impact of automation on business continuity."
	"The integration of 'Optimization and scaling' with 'Improvement' is key to maximizing the return on investments in automation. It ensures that improvements are not isolated but contribute to the overall scalability and optimization of automation solutions. This holistic approach enhances the value derived from automation in terms of business continuity."
	"Both clauses are compatible."
	"By combining 'Optimization and Scaling' with 'Improvement,' we future-proof automation initiatives. This integration ensures that automation solutions are effective today and designed to adapt and grow with the organization. It provides a strategic advantage in maintaining business continuity in a constantly evolving business landscape."
	"This is a key area of the broad diagram presented. Besides linking both rules, the ISO 22301 clause expands the scope by introducing the scaling area. Nonetheless, both converge in fighting (e.g.), Non-Conformities."
	"If 'Optimization and scaling' are aligned with 'Improvement,' it will support the strategic evolution of automation capabilities. This integration enables organizations to also refine existing processes and scale automation efforts to cover broader areas. It ensures that improvements in automation contribute directly to enhancing business continuity strategies."
	"It establishes a framework for iterative enhancement. This combination ensures that automation solutions are optimized for current operations and scalable to accommodate future needs. It promotes a culture of continuous improvement, driving sustained benefits for business continuity."
Q8.	"This approach ensures a robust and holistic understanding of the integration of ISO 22301 and IEEE 2755.2, drawing on the expertise of practitioners and leveraging existing organizational documentation for added context and validation".
	"As I had the opportunity to cover previously (above), the match identified between the ISO 22301 Clauses and the IEEE 2755.2is indeed very strong and, most importantly, extremely relevant. Taking that and to conclude, in my opinion, the design of this framework should constitute a very useful and powerful tool for, mainly, to have the right management tool to obtain success in complex projects."
	"In my view, the main advantage is the ease of understanding the process and reading the ISO clauses and stages. This model makes it easier for business specialists to have a clearer model."
	"One notable advantage is the seamless alignment of organizational context with operational structures. This provides a solid foundation for BCM and IPA initiatives, ensuring that automation efforts are strategically deployed in areas with the highest impact on business continuity."
	"The combination of framework ISO 22301 and IEEE 2755.2 has the potential to revolutionize the way organizations approach business continuity and automation. By leveraging the strengths of both frameworks, organizations can achieve a more resilient and efficient operational model that enhances their ability to navigate disruptions and drive sustainable growth. But in terms of implementation, it's imperative to have a robust change management process in place to ensure a smooth transition. Stakeholders buy-in and training will play a crucial role in maximizing the benefits of this integrated approach."
	"The integration of clauses from ISO 22301 and IEEE 2755.2 holds significant potential in reshaping the intersection of Business Continuity Management (BCM) and Intelligent Process Automation (IPA). By combining these frameworks, we create a comprehensive approach that safeguards critical business functions during disruptions and not leverages automation to enhance operational efficiency."

significant potential in reshaping the intersection of BCM and IPA. The combined framework is a powerful tool that can revolutionize how organizations approach BC and automation. Four of these six responses express positive views regarding the integration of ISO 22301 and IEEE 2755.2, highlighting advantages such as enhanced understanding, strong relevance, ease of comprehension, and potential for revolutionizing BC and automation. One response emphasizes the importance of change management for successful implementation. One provides a practical insight into how the combined framework can be a powerful management tool for complex projects.

Please note that this analysis is based on a qualitative evaluation of the responses, as the provided answers are not quantifiable in a traditional percentage format.

Overall, the feedback reflects a positive outlook on integrating ISO 22301 and IEEE 2755.2. Practitioners and experts see this combined framework as a valuable approach that has the potential to significantly impact the intersection of BCM and IPA positively. They recognize its potential to enhance organizational resilience and efficiency in the face of disruptions. However, they also acknowledge the importance of careful implementation, particularly in terms of change management and stakeholder buy-in

IX. CONCLUSION

This research provides an approach to a bi-directional mapping for IEEE 2755.2:2020 and ISO 22301:2019 on their clauses and sub-clauses (stages regarding the IEEE 2755.2:2020 standard). In addition to the mapping exercise, our objective is to augment the utility of IEEE 2755.2:2020 and ISO 22301:2019 by introducing visual models as a complementary aid to their existing textual representation.

This document offers versatile applications, serving organizations, projects, acquirers, and suppliers in diverse capacities. For academia, this research provides an instrumental resource for studying and advancing the integration of IPA and BCMS. Professionals stand to benefit from the practical insights and guidelines offered for implementing these frameworks in real-world scenarios.

However, it's important to acknowledge the limitations of this study. Contextual variations among organizations may require tailored approaches not covered in this analysis. Additionally, evolving industry standards and technologies could necessitate ongoing adaptation.

Looking ahead and charting a course for future research, a critical area of exploration involves the development of a comprehensive Maturity Model for both IEEE 2755.2:2020

and ISO 22301:2019, connected to essential domains including cybersecurity, data breach prevention, governance, risk, and compliance. The aim is to gain insights into the comprehensive impact on people, technology, and processes. Such a model would capture the nuances of individual and organizational contexts and provide a nuanced evaluation of the maturity of implementing SBIPA under the purview of BCMS. This framework becomes pivotal in offering organizations a structured approach to gauge their maturity levels, fostering continuous improvement and resilience in the face of evolving challenges.

Moreover, pursuing a sustainable combination of IEEE 2755:2020 and ISO 22301:2019 demands a multifaceted approach. Beyond the technical integration, prioritizing energy efficiency, actively reducing the carbon footprint, and promoting inclusivity within the framework emerge as integral components. A meticulous cost-benefit analysis, coupled with a commitment to adaptability in the face of future technological advancements, forms the basis for a resilient and sustainable merged framework.

Compliance with stringent environmental standards becomes very important, and ongoing stakeholder engagement, transparent communication, and a culture of continuous improvement further solidifies the alignment with sustainable practices in business continuity and intelligent process automation.

APPENDIX A

See Table 7.

APPENDIX B

See Table 8.

APPENDIX C

See Table 9.

REFERENCES

[1] S. Chatterjee, R. Chaudhari, and R. Shams, "Applications of industry 4.0 for pandemic responses and business Continuity: A TOE-DCV integrated approach," *IEEE Trans. Eng. Manag.*, early access, Mar. 17, 2023, doi: 10.1109/TEM.2023.3250587.

[2] M. Röglinger, R. Plattfaut, V. Borghoff, G. Kerpedzhiev, J. Becker, D. Beverungen, J. vom Brocke, A. Van Looy, A. del-Río-Ortega, S. Rinderle-Ma, M. Rosemann, F. M. Santoro, and P. Trkman, "Exogenous shocks and business process management: A scholars' perspective on challenges and opportunities," *Bus. Inf. Syst. Eng.*, vol. 64, no. 5, pp. 669–687, Oct. 2022, doi: 10.1007/s12599-021-00740-w.

[3] M. Greve, S. Hengstler, and S. T. N. Trang. (2020). *Overcoming Digital Challenges: A Cross-Cultural Experimental Investigation of Recovering From Data Breaches*. Accessed: Nov. 19, 2023. [Online]. Available: https://www.researchgate.net/publication/344367508

[4] D. A. da Silva Costa, H. Sito Mamede, and M. M. da Silva, "Robotic process automation (RPA) adoption: A systematic literature review," *Eng. Manage. Prod. Services*, vol. 14, no. 2, pp. 1–12, Jun. 2022, doi: 10.2478/emj-2022-0012.

[5] R. Uskenbayeva, Z. Kalpeyeva, R. Satybaldiyeva, A. Moldagulova, and A. Kassymova, "Applying of RPA in administrative processes of public administration," in *Proc. IEEE 21st Conf. Bus. Informat. (CBI)*, vol. 2, Jul. 2019, pp. 9–12, doi: 10.1109/CBI.2019.10089.

[6] S. Sutipitakwong and P. Jamsri, "The effectiveness of RPA in fine-tuning tedious tasks," in *Proc. 6th Int. Conf. Eng., Appl. Sci. Technol. (ICEAST)*, Jul. 2020, pp. 1–4, doi: 10.1109/ICEAST50382.2020.9165452.

[7] T. Chakraborti, *From Robotic Process Automation to Intelligent Process Automation: Emerging Trends*. Cham, Switzerland: Springer, 2020, doi: 10.1007/978-3-030-58779-6.

[8] Angraini, R. A. Alias, and Okfalisa, "Information security policy compliance: Systematic literature review," *Proc. Comput. Sci.*, vol. 161, pp. 1216–1224, Jan. 2019, doi: 10.1016/j.procs.2019.11.235.

[9] S. E. A. Ali, F.-W. Lai, P. D. D. Dominic, N. J. Brown, P. B. B. Lowry, and R. F. Ali, "Stock market reactions to favorable and unfavorable information security events: A systematic literature review," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102451, doi: 10.1016/j.cose.2021.102451.

[10] S. Rasoulian, Y. Grégoire, R. Legoux, and S. Sénécal, "Service crisis recovery and firm performance: Insights from information breach announcements," *J. Acad. Marketing Sci.*, vol. 45, no. 6, pp. 789–806, Nov. 2017, doi: 10.1007/s11747-017-0543-8.

[11] *2755.2-2020—IEEE Recommended Practice for Implementation and Management Methodology for Software-Based Intelligent Process Automation | IEEE Standard | IEEE Xplore*. Accessed: Apr. 7, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9404959

[12] (2020). *ISO 22313:2020(en) Security and Resilience—Business Continuity Management Systems—Guidance on the Use of ISO 22301*. Accessed: Feb. 25, 2023. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-2:v1:en

[13] N. C. Suresh, G. L. Sanders, and M. J. Braunscheidel, "Business continuity management for supply chains facing catastrophic events," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 129–138, 3rd Quart., 2020, doi: 10.1109/EMR.2020.3005506.

[14] J. Brás, R. Pereira, and S. Moro, "Intelligent process automation and business continuity: Areas for future research," *Information*, vol. 14, no. 2, p. 122, Feb. 2023, doi: 10.3390/info14020122.

[15] (2012). *ISO 22301:2012(en), Societal Security—Business Continuity Management Systems—Requirements*. Accessed: Feb. 23, 2023. [Online]. Available: https://www.iso.org/obp/ui/#iso: std: iso:22301:ed-1:v2:en

[16] *Standards—BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR)*. Accessed: Feb. 23, 2023. [Online]. Available: https://www.bcmpedia.org/wiki/Standards

[17] ISO. (2019). *ISO 22301:2019 Security and Resilience—Business Continuity Management Systems—Requirements*. Accessed: Dec. 26, 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso: std: iso:22301:ed-2:v1:en

[18] *PAS56, PAS 56 and BS25999 Business Continuity Management*. Accessed: Feb. 23, 2023. [Online]. Available: https://web.archive.org/web/20061015195120/http://www.pas56.com/

[19] *ISO/IEC 27001:2022—Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*. Accessed: Apr. 2, 2023. [Online]. Available: https://www.iso.org/standard/82875.html

[20] *BS25999, BS 25999*. Accessed: Apr. 4, 2023. [Online]. Available: https://web.archive.org/web/20061015195123/http://www.pas56.com/support.htm

[21] *BS 25999 and Its Contribution to Business Continuity Management | BSI Middle East and Africa*. Accessed: Apr. 4, 2023. [Online]. Available: https://www.bsigroup.com/en-AE/About-BSI/Media-Center/Press-releases/2011/6/BS-25999-and-its-Contribution-to-Business-Continuity-Management/

[22] *Moving From BS 25999-2 to ISO 22301*. Accessed: Apr. 4, 2023. [Online]. Available: https://www.bsigroup.com/documents/iso-22301/resources/bsi-bs25999-to-iso22301-transition-uk-en.pdf

[23] *SI 24001: Organizational Resilience Management System (ORMS)—Requirements and Guidance for Use—Standards Institution of Israel*. Accessed: Apr. 2, 2023. [Online]. Available: https://www.sii.org.il/en/24001

[24] *ISO/PAS 22399:2007—Societal Security—Guideline for Incident Preparedness and Operational Continuity Management*. Accessed: Apr. 2, 2023. [Online]. Available: https://www.iso.org/standard/50295.html

[25] *Singapore Standards*. Accessed: Apr. 2, 2023. [Online]. Available: https://www.singaporestandardseshop.sg/Product/SSPdtDetail/235b31c7-7d39-4282-9205-6e4a5a3f7805

[26] NFPA. (Dec. 17, 2012). *NFPA® 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2013 Edition An International Codes and Standards Organization*. Accessed: Feb. 22, 2023. [Online]. Available: http://www.nfpa.org

[27] *Business Continuity-Managing Disruption-Related Risk*. Accessed: Apr. 4, 2023. [Online]. Available: http://www.saiglobal.com.au

[28] *ASIS International and BSI Release Joint Business Continuity Management ANSI Standard*. Accessed: Apr. 2, 2023. [Online]. Available: https://www.continuitycentral.com/news05526.html

[29] *Business Continuity Management: Understanding the Requirements of ISO 22301:2012 and ISO 22301:2019*, BSI Org., Standard ISO 22301, 2019.

[30] *ISO 22301, The Business Continuity Management Standard*. Accessed: Apr. 2, 2023. [Online]. Available: https://www.isms.online/iso-22301/

[31] *NIST SP 800-34 | NIST*. Accessed: Apr. 4, 2023. [Online]. Available: https://www.nist.gov/privacy-framework/nist-sp-800-34

[32] *IEEE Recommended Practice for Implementation and Management Methodology for Software-Based Intelligent Process Automation*, Ted Burse, Bursa, Türkiye, 2020.

[33] (Jan. 2017). *P2755/D1, IEEE Approved Draft Guide to Terms and Concepts in Intelligent Process Automation*. [Online]. Available: https://ieeexplore.ieee.org/document/7891875/keywords#keywords

[34] *ISO/IEC 15504-2:2003—Information Technology—Process Assessment—Part 2: Performing an Assessment*. Accessed: Apr. 7, 2023. [Online]. Available: https://www.iso.org/standard/37458.html

[35] *ISO/IEC TR 18018:2010—Information Technology—Systems and Software Engineering—Guide for Iguration Management Tool Capabilities*. Accessed: Apr. 7, 2023. [Online]. Available: https://www.iso.org/standard/51042.html

[36] *ISO/IEC 33020:2015—Information Technology—Process Assessment—Process Measurement Framework for Assessment of Process Capability*. Accessed: Apr. 7, 2023. [Online]. Available: https://www.iso.org/standard/54195.html

[37] *IEEE Guide for Terms and Concepts in Intelligent Process Automation*, Standard IEE 2755-2017, 2017.

[38] *2755.1-2019—IEEE Guide for Taxonomy for Intelligent Process Automation Product Features and Functionality | IEEE Standard | IEEE Xplore*. Accessed: Apr. 7, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/8764094

[39] *PDSA Cycle—The W. Edwards Deming Institute*. Accessed: Feb. 21, 2023. [Online]. Available: https://deming.org/explore/pdsa/

[40] J. Ning, Z. Chen, and G. Liu, "PDCA process application in the continuous improvement of software quality," in *Proc. Int. Conf. Comput., Mechatronics, Control Electron. Eng.*, vol. 1, Aug. 2010, pp. 61–65. Accessed: Feb. 21, 2023. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5609635

[41] J. Järveläinen, "IT incidents and business impacts: Validating a framework for continuity management in information systems," *Int. J. Inf. Manage.*, vol. 33, no. 3, pp. 583–590, Jun. 2013, doi: 10.1016/j.ijinfomgt.2013.03.001.

[42] *P2755.2/D2, Sept_2020-IEEE Approved Draft Recommended Practice for Implementation and Management Methodology for Software Based Intelligent Process Automation (SBIPA)*, Standard IEEE P2755.2/D2, Sep. 2020, pp. 1–58. Accessed: Mar. 17, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9190584

[43] *IEEE Guide for Terms and Concepts in Intelligent Process Automation*, IEEE Standard 2755-2017, 2017, pp. 1–16, doi: 10.1109/IEEESTD.2017.8070671.

[44] T. Hollweck, "Robert K. Yin. (2014). Case study research design and methods (5th ed.)," *Can. J. Program Eval.*, vol. 30, no. 1, pp. 108–110, Mar. 2015, doi: 10.3138/cjpe.30.1.108.

[45] K. M. Eisenhardt, "Building theories from case study research," *Acad. Manage. Rev.*, vol. 14, no. 4, pp. 532–550, Oct. 1989. [Online]. Available: https://www.jstor.org/stable/258557

[46] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decis. Support Syst.*, vol. 15, no. 4, pp. 251–266, Dec. 1995, doi: 10.1016/0167-9236(94)00041-2.

[47] M. Rosemann and I. Vessey, "Toward improving the relevance of information systems research to practice: The role of applicability checks," *MIS Quart.*, vol. 32, no. 1, p. 1, 2008, doi: 10.2307/25148826.

[48] *ISO 22301: Business Continuity Management System, Implementation and Audit | Groups | LinkedIn*. Accessed: Aug. 19, 2023. [Online]. Available: https://www.linkedin.com/groups/8347186/

[49] *Institute of Business Continuity Management | Groups | LinkedIn*. Accessed: Jul. 7, 2023. [Online]. Available: https://www.linkedin.com/groups/4699159/

[50] *Business Continuity | Groups | LinkedIn*. Accessed: Oct. 7, 2023. [Online]. Available: https://www.linkedin.com/groups/60416/

[51] *Institute of Business Continuity Management | Groups | LinkedIn*. Accessed: May 22, 2023. [Online]. Available: https://www.linkedin.com/groups/4699159/

[52] *Business Continuity & Disaster Recovery Consultants | Groups | LinkedIn*. Accessed: Jun. 17, 2023. [Online]. Available: https://www.linkedin.com/groups/126477/

[53] *ISO 22301: Business Continuity Management System, Implementation and Audit | Groups | LinkedIn*. Accessed: Sep. 5, 2023. [Online]. Available: https://www.linkedin.com/groups/8347186/

[54] *Disaster Recovery Journal (DRJ) Dedicated to Business Continuity Since 1987 | Groups | LinkedIn*. Accessed: Jun. 5, 2023. [Online]. Available: https://www.linkedin.com/groups/117659/

[55] *RPA & IPA / AI+ML / IDP / BPM ? Consultants Group | Groups | LinkedIn*. Accessed: Oct. 7, 2023. [Online]. Available: https://www.linkedin.com/groups/7045359/

[56] *Robotic Process Automation (RPA) / IPA / Artificial Intelligence / Machine Learning / Analytics | Groups | LinkedIn*. Accessed: Oct. 7, 2023. [Online]. Available: https://www.linkedin.com/groups/8604621/

[57] M. D. Myers and M. Newman, "The qualitative interview in IS research: Examining the craft," *Inf. Org.*, vol. 17, no. 1, pp. 2–26, Jan. 2007, doi: 10.1016/j.infoandorg.2006.11.001.

[58] M. D. Myers, *Qualitative Research in Business and Management*, 2nd ed. Newbury Park, CA, USA: Sage, 2013.

[59] I. S. Bianchi, R. D. Sousa, and R. Pereira, "Information technology governance for higher education institutions: A multi-country study," *Information*, vol. 8, no. 2, p. 26, 2021, doi: 10.3390/informatics8020026.

JOSÉ CASCAIS BRÁS received the B.S. degree in information technology management and the master's degree in software engineering from Universidade Lusófona, Lisbon, Portugal, in 2010 and 2017, respectively. He is currently pursuing the Ph.D. degree in information science and technology with the ISCTE University of Lisbon, Portugal.

He is also a Research Assistant Professor with ISTAR-IUL—Information Sciences, Technologies and Architecture Research Center (ISTA), ISCTE University of Lisbon, and a Research Assistant Professor with COPELABS, Universidade Lusófona. He is also the Consulting Director of CGI, Portugal. His research interests include business continuity, governance, risk, compliance, the intersection between business process management, business process automation, intelligent process automation, and business continuity. More specifically, his research seeks to understand the state of awareness of RPA/IPA within the business continuity management lifecycle.

RUBEN FILIPE PEREIRA received the master's degree in computer engineering and in computer science and the Ph.D. degree in computer science and information systems from Instituto Superior Técnico. He is currently an Assistant Professor with ISCTE. With extensive experience as a consultant in various sectors, including services, banking, telecommunications, healthcare, and e-commerce. Currently, he is an Advisor to several prominent organizations. He is also a Researcher with the Institute of Telecommunications and leads a research group with INOV. With over 2000 citations, he is a recognized author of numerous scientific articles in areas, such as IT risk, IT strategy, IT value, IT governance, business process management, innovation, digital transformation, DevOps, and robotic process automation.

SÉRGIO MORO is currently a Full Professor with ISCTE, where he is also the Vice-President of the Scientific Council. He is also the former Deputy Director of the ISTAR Research Center, where he coordinated the Information Systems Group. He is also an Interdisciplinary Data Scientist that envisions the development of innovative predictive systems through data science approaches in distinct domains, such as marketing, management, tourism, and education. His work has received more than 2600 Scopus (H-index—25) and more than 4800 Google Scholar (H-index—33) citations. He is also the Deputy Director of the Department of Information Science and Technology. He is also the Director of the Master in Data Science.

ISAIAS SCALABRIN BIANCHI received the Ph.D. degree in technology and systems information from the University of Minho, Portugal. He is currently a Civil Servant with the Federal University of Santa Catarina, where he has been working, since 2010, holding several management positions. He investigates IT governance, information technology services management, business process management, business intelligence, and digital transformation and innovation, in particular for public organizations and higher education institutions. His research has been published in leading IS conferences and international journals. He is also an Assistant Coordinator with the Open University of Brazil—UAB and Federal University of Santa Catarina, where he is also a Professor with the Master Program in Management. He is also a Visiting Professor with Al-Farabi Kazakh National University teaching and supervising Ph.D. students in the topics of digital transformation, digital marketing, and supply chain management. He also co-supervises master's students with the University of Minho and Instituto Universitário de Lisboa. He has achieved the Moodle Educator Competence in the Moodle Educator Certification Program.

RUI RIBEIRO received the Ph.D. degree in applied business management and in information systems from ISCTE/IUL, the M.B.A. degree from Universidade Católica Portuguesa, and the degree in computer engineering from IST. In academia, he is currently the Executive Director of the Lusofona Information Systems School—LISS and a Professor with Universidade Lusófona. At a business level, he is also the Head of Consulting and Technology with Auren Portugal, having previously been the General Director of IPTelecom, the Commercial Director of Infraestruturas de Portugal S.A., the Director of Information Systems with EP—Estradas de Portugal S.A., and the Professional Services Manager of Sybase Inc., Portugal. He is the coauthor of the book *Digital Transformation: The Challenges, Thinking and Doing* and several scientific articles, including *Digital Transformation: The Evolution of the Enterprise Value Chain* Series on Advances in Intelligent Systems and Computing (2020), pp. 290-302.

Chapter 4

Article nr. #3 – “Advances in Auditing and Business Continuity: A Study in Financial Companies”

This article provides crucial insights into the integration of IPA within business continuity auditing, specifically focusing on the Portuguese banking sector. The research offers a detailed analysis of how automation is transforming the audit process, emphasizing its importance for reinforcing operational efficiency and enhancing cost savings. It underscores the pivotal role of auditors in navigating technological advancements to safeguard business continuity. By introducing a comprehensive application that automates critical audit activities, such as communication, information requests, and final report submissions, the study demonstrates how automation can liberate auditors from routine tasks. The incorporation of business intelligence further enhances this automation framework, enabling a meticulous analysis of key performance indicators within audit departments.

The article serves as an essential contribution to understanding the transformative potential of automation in auditing. It provides a replicable framework for organizations aiming to strengthen their business continuity efforts through technological integration. By focusing on the Portuguese banking sector, the study offers empirical insights into how automation supports decision-making processes, improves operational resilience, and alleviates auditors from repetitive tasks.

Article Details:

- Title: "Advances in Auditing and Business Continuity: A Study in Financial Companies."
- Journal: Journal of Open Innovation: Technology, Market, and Complexity (JOItmC) (ISSN 2199-8531)
- Date: 05/16/2024
- Scimago Journal Rank: Quartile 1 - Business and Management
- Publisher: Elsevier

Journal of Open Innovation: Technology, Market, and Complexity 10 (2024) 100304

Contents lists available at ScienceDirect

Journal of Open Innovation: Technology, Market, and Complexity

journal homepage: www.sciencedirect.com/journal/journal-of-open-innovation-technology-market-and-complexity

Advances in auditing and business continuity: A study in financial companies

José Cascais Brás [a,e,*], Ruben Filipe Pereira [b], Micaela Fonseca [c], Rui Ribeiro [a], Isaias Scalabrin Bianchi [d]

[a] Universidade Lusófona, COPELABS, Lisboa, Portugal
[b] Instituto de Telecomunicações, Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal
[c] Instituto Universitário de Lisboa (ISCTE-IUL), Portugal
[d] Federal University of Santa Catarina, Brasil
[e] CGI Innovation Hub Lisbon, Lisboa, Portugal

ARTICLE INFO

Keywords:
Business continuity
Governance
Risk
Compliance
Auditing
Robotic process automation
Intelligent process automation
Business process management

ABSTRACT

This paper delves into the integration of Intelligent Process Automation within the domain of business continuity auditing, with a focus on the Portuguese banking sector. In an era marked by rapid technological advancement, organizations are increasingly leveraging automation to reinforce operational efficiency and realize substantial cost savings. Concurrently, auditors play a pivotal role in ensuring seamless transitions amid technological transformations to safeguard business continuity. This research endeavors to bridge the realms of business continuity and intelligent automation, culminating in a comprehensive application that streamlines the audit process. The implemented solution encompasses the automation of critical audit activities, including communication, information requests, and final report submissions, liberating auditors from the chains of repetitive tasks. The incorporation of business intelligence augments this automation framework, enabling a meticulous analysis of key performance indicators within the audit department. This ensures a continuous evaluation of the efficacy of the Annual Audit Plan. Empirical validation of this initiative was achieved through surveys conducted with audit teams from four prominent Portuguese banks. The results unequivocally affirm the potential benefits of this implementation, extending invaluable support to management in the decision-making process, while concurrently alleviating auditors of routine tasks inherent to the audit process. This study not only underscores the transformative potential of intelligent process automation in the audit domain but also offers a replicable framework for organizations seeking to fortify their business continuity efforts through technological integration. The findings hold implications for businesses navigating the dynamic intersection of technology and audit practices, providing a blueprint for harnessing automation for enhanced operational resilience.

1. Introduction

Technological advancements have greatly increased information accessibility and are continuously reshaping information systems to meet future demands This dynamic environment compels organizations to adopt open innovation strategies to streamline operations, enhance efficiencies, and fortify fraud prevention measures. The COVID-19 pandemic has accelerated the shift towards remote work, emphasizing the importance of process automation. In auditing, technology has become essential in ensuring compliance, assessing risks, and improving operational efficiencies, promoting transparency and accountability. The shift from manual to automated and continuous auditing is driven by emerging technologies like Artificial Intelligence (AI) and blockchain, significantly affecting the banking sector. Despite these advances, the transition to fully digital auditing practices remains gradual, with many institutions still reliant on traditional methods.

The auditing process has evolved from traditional manual audits of paper documentation to computer-based auditing, progressing towards a paperless, electronic, real-time continuous auditing environment (Rezaee et al., 2002). The banking sector has faced numerous challenges in recent years, responding to incentives and imperatives related to technological advances, market volatility, and increasing regulatory and

* Corresponding author at: Universidade Lusófona, COPELABS, Lisboa, Portugal.
E-mail address: jose_manuel_bras@iscte.iul (J.C. Brás).

https://doi.org/10.1016/j.joitmc.2024.100304
Received 14 January 2024; Received in revised form 12 May 2024; Accepted 16 May 2024
Available online 19 May 2024

public scrutiny. Since the 2007 financial crisis, known as the subprime crisis, the audit function in banking institutions has become significantly more crucial. Its primary mission is to mitigate the risk of potential or actual losses, thereby enhancing the institution's risk profile (Zinca, 2016). Internal Audit (IA) departments are under increasing pressure to leverage technology for automating the identification of exceptions and/or anomalies and for control testing (The Institute of Internal Auditors, 2019).

Despite the pervasive integration of digital tools into daily life and advancements in various sectors, the application of digital technologies in auditing is still in its nascent stages (Vasarhelyi et al., 2012). Internal Audit Functions (IAFs) predominantly adhere to traditional auditing approaches, and the transition to the continuous audit paradigm has not yet been fully realized in most organizations (AUDITBOARD, 2018; Skantze, 2017).

In the dynamic landscape of technological advancement, businesses find themselves in a race against time to implement automated systems and harness cutting-edge technologies (Mamede et al., 2023). This not only amplifies operational efficiency but also amplifies service effectiveness and drives substantial cost savings, all while ensuring the uninterrupted flow of critical services (J. Brás et al., 2023). Simultaneously, auditors stand as vigilant sentinels, poised to navigate the currents of global change (Murphy, 2020) and scrutinize the orchestration of business continuity processes (Wojciechowska-Filipek, 2019; J. C. Brás et al., 2023; Brás and Guerreiro, 2016).

Sophisticated algorithms employed by modern systems offer a proactive enhancement to banks' capacities for safeguarding operations and reputation. This strategic adoption facilitates navigation through the volatile business landscape, preemptively identifying vulnerabilities before they escalate into significant threats (V-Soft Consulting, 2020). Financial institutions harness such tools for predictive credit risk analysis, leveraging extensive data to forecast market risks and potential loan defaults. Such initiatives underscore the institutions' commitment to risk management, providing a competitive edge in strategic foresight (Anagnoste, 2017; Steinhoff et al., 2018).

Robotic Process Automation (RPA) exemplifies the forefront of technological integration in business processes, augmenting human capabilities and redefining audit procedures without replacing human roles (Devarajan, 2018). RPA, building on the technological innovations of the 1990s, including screen scraping and AI, is transforming into a formidable force (Issa et al., 2016; Javatpoint, 2021). When combined with Intelligent Automation to create Intelligent Process Automation (IPA), RPA significantly raises the quality of auditing, enhancing anomaly detection and insight discovery (Chambers, 2020; Handoko et al., 2021a; Lievano-Martínez et al., 2022; Minnaar and Smith, 2018; Mittal, 2021).

The advancement toward automation-intensive auditing, propelled by open innovation, suggests a diminishing role for manual processes. Collaborative efforts in technology development and knowledge sharing can further streamline audit methodologies (Lu and Chesbrough, 2021; Peñarroya-Farell et al., 2021). Effective utilization of automation in auditing, bolstered by open innovation strategies, can yield outstanding results. Encouraging broader collaboration and external inputs ensures that decisions regarding its implementation are made with discernment, leveraging diverse expertise for enhanced decision-making. (Bedard et al., 2006; David Audretsch and Belitski, 2022; Julka, 2021; Majchrzak et al., 2023). With the automation technology market expected to grow exponentially, the incorporation of automation in strategic planning is imperative. (Agoglia et al., 2010; Devarajan, 2018; Raval and Smith, 2020). Projections indicate that the global automation technology market is poised to attain a substantial valuation of $25.66 billion by 2027, characterized by a robust compound annual growth rate of 40.6 percent (Sikora et al., 2019).

Auditors are tasked with discerning the tasks suitable for automation, mitigating risks associated with automation, and ensuring robots' behavior aligns with societal norms and human preferences (Alles and Kogan, 2008; Moffitt et al., 2018a). Future auditors must transcend traditional roles, integrating mature automated processes, standardized definitions, and adept management to add value and competitive advantage (Bharadhwaj, 2021; Griffiths and Pretorius, 2021; Moffitt et al., 2018a; Vasarhelyi et al., 2004).

RPA's implementation extends beyond technological deployment, involving process optimization and the integration of cognitive capabilities into machines (Syed et al., 2020; Appelbaum and Nehmer, 2017; Vlăduţ et al., 2018). Despite RPA and AI's benefits, it's crucial to acknowledge and navigate the associated challenges and risks to prevent systemic lapses and ensure continued accuracy and efficiency in response to business process changes (Aksoy and Hacioglu, 2021; Gotthardt et al., 2020; Issa et al., 2016; Mandal et al., 2017).

In resume, RPA introduces various risks despite its efficiency benefits, including security vulnerabilities as bots access sensitive data, which may lead to breaches if not securely managed (J. Brás et al., 2023). Operational risks also arise from potential software bugs and maintenance issues, particularly when RPAs are not updated in line with evolving business processes, leading to failures and disruptions. Additionally, compliance risks are significant, as improper programming or oversight might result in regulatory breaches, inviting leg (Deloitte, 2018; Joshi, 2019; Mennen and Van Tuyll, 2015; Szalony et al., 2019), and penalties and reputational damage. Scaling RPAs can compound these issues, making bot management increasingly complex and challenging (Durst and Henschel, 2020; KPMG, 2018a; Olson and Wu, 2021; Pluzhnikov, 2020; Violino, 2020). Over-dependence on automation can reduce human oversight, critical in decision-making processes, potentially affecting operational integrity if RPAs fail. Furthermore, job displacement from automation can impact employee morale and lead to resistance, necessitating careful management and retraining programs to ensure workforce adaptation and acceptance. Effective risk mitigation requires robust governance, continuous monitoring, and integration of RPAs into broader Information Technology (IT) and business strategies to balance benefits against potential downsides(Deloitte, 2020; ELEKS, 2022; Hugo Ciopages, 2016; Namchoochai et al., 2020).

With the imperative to automate audit operations as a guiding principle, this study embarks on a mission to mechanize manual and repetitive activities within the audit process (Nunes et al., 2020). This endeavor promises to underpin a more effective business continuity management, facilitating the identification of optimal solutions while mitigating potential risks (Bharadhwaj, 2021; J. C. Brás et al., 2023; Handoko et al., 2021a). In essence, this reconfiguration of the auditor's role envisages a pivot toward the assessment facet of audit procedures, liberating valuable time from the clutches of routine tasks (Huang and Vasarhelyi, 2019; Moffitt et al., 2018a).

This research aims to rigorously assess whether RPA and IPA can refine the audit process and if active monitoring of audit plans can bolster decision-making. Hence, this article aims to focus on two main research questions:

1. Can RPA and IPA improve the audit process?
2. Can active monitoring of audit plans improve decision-making?

2. Research methodology

In the pursuit of this study, a research approach founded on the principles of the Design Science Research Method (DSRM) is adopted. This method is instrumental in addressing complex issues through the creation of novel artifacts, evaluating their designs, and effectively disseminating the findings to pertinent stakeholders (Hevner et al., 2004; Peffers et al., 2006).

The DSRM framework encompasses five key stages, delineated as follows:

1. Problem identification and motivation: This initial phase involves the discernment of a specific research conundrum and the elucidation of the inherent value in proffering a solution. This serves to

engender motivation, both for the researcher and the wider research community, to ardently pursue the resolution of said problem.

2. Objectives of a solution: After the delineation of the problem, this stage demands the establishment of precise goals for the envisaged solution. These objectives are logically derived from the foundational problem definition, anchoring the subsequent development process.

3. Design and development: This pivotal stage entails the actualization of the solution. Here, the desired functionality and architectural attributes of the artifact are meticulously delineated, culminating in the construction of the artifact itself.

4. Demonstration: In this conclusive phase, the efficacy of the artifact in addressing the identified problem is validated. This entails subjecting it to rigorous experimentation, simulations, or other pertinent evaluative activities, thereby substantiating its effectiveness.

5. Evaluation: This critical phase entails a comprehensive assessment of the created artifact's efficacy in resolving an authentic problem and its practical utility. This involves subjecting the artifact to rigorous testing, simulations, or real-world applications to gauge its performance, reliability, and applicability in practical scenarios. The evaluation process serves as a pivotal validation of the artifact's real-world relevance and its potential to address genuine issues in practice. Fig. 1 presents a description of the research strategy using a DSRM process and summarizes the design and development of the artifact under analysis.

By adhering to the systematic rigor of the DSRM framework, this research endeavors to navigate the intricate terrain of problem-solving, thereby yielding insights that contribute substantively to the body of knowledge in the field.

The adoption of the DSRM approach in the realm of engineering and related themes offers significant advantages, primarily in terms of practical applicability (Peffers et al., 2007). Furthermore, this methodology exhibits a commendable degree of adaptability. Although the model is ostensibly structured in a sequential manner, researchers possess the flexibility to initiate their efforts at any juncture within activities one, two, three, or four. This adaptability caters to individual researchers' specific approaches and requirements (Maria Gonçalves Martins et al., 2018).

The main objectives of the proposed solution include strict compliance with and timely updates to the Annual Audit Plan. It aims to simplify routine tasks such as scheduling meetings and sending emails, thereby freeing up resources for more strategic activities. Additionally, the solution will evaluate auditor performance, providing insights that help pinpoint opportunities for improvement and refinement (Dabthong et al., 2021). Fig. 2 illustrates the six key activities facilitated by the potential automation solution.

Next, the IPA system will issue timely alerts to auditors, informing them of upcoming audits and requesting their permission to proceed. This enhances the efficiency of the audit initiation and ensures better time management.

The system will also automate the creation of emails and meeting requests, which are recurrent tasks within the audit process, thus enhancing operational efficiency.

After an audit is completed, the final report is meticulously analyzed using CV techniques again. This analysis provides critical data necessary for developing Key Performance Indicators (KPIs), which will be further discussed.

Given these activities, choosing the right RPA tool is crucial. As shown in Table 1, UiPath stands out for its cost-effectiveness and extensive support and learning community, making it the preferred tool for developing the automation framework.

In addition to the UI Path tool, integrating a Business Intelligence (BI) tool like Power BI is essential for enhancing the internal audit function's effectiveness and aligning it with organizational goals. This integration is crucial for assessing audit performance, which is increasingly scrutinized by regulators and investors concerning an organization's operational integrity. Power BI will be used to visualize KPIs identified by leading research institutions and regulatory bodies,

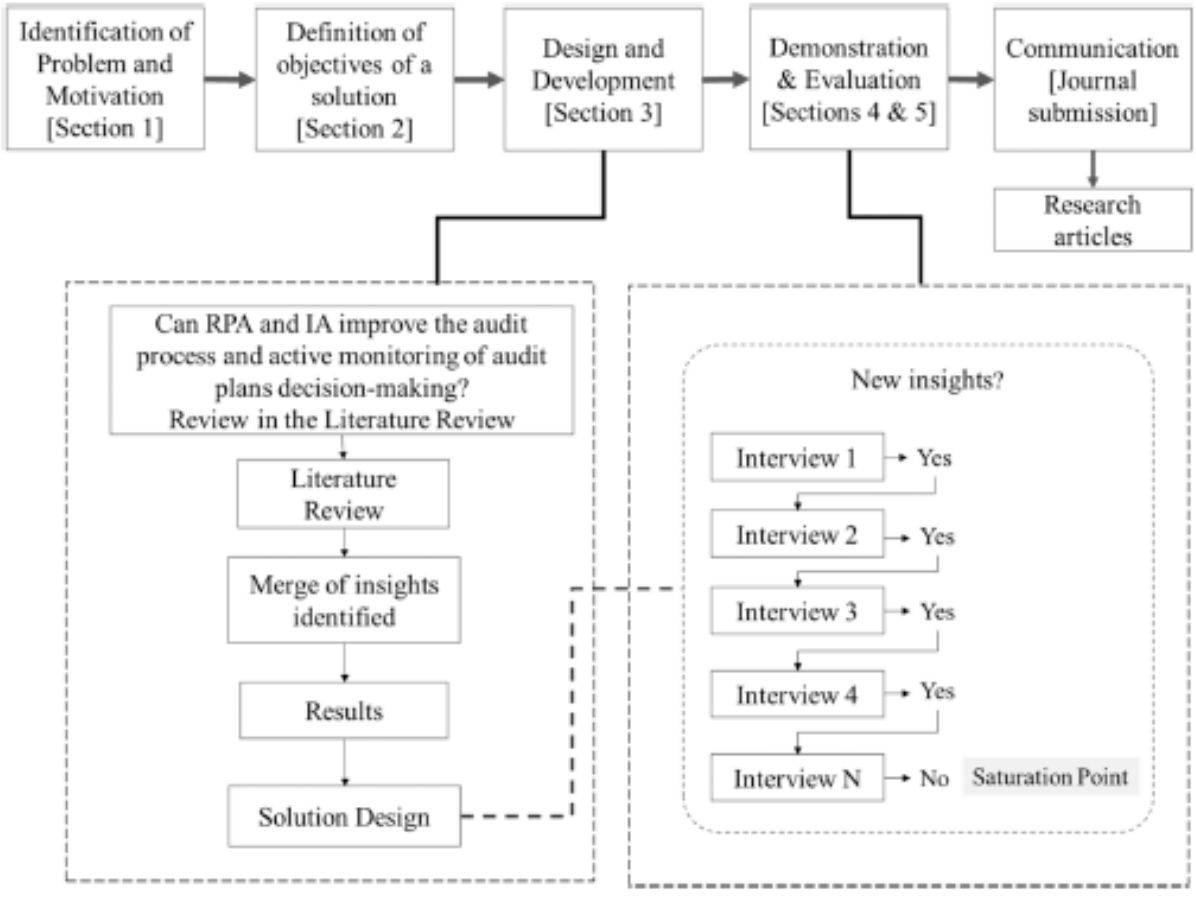


Fig. 1. DSRM workflow diagram.

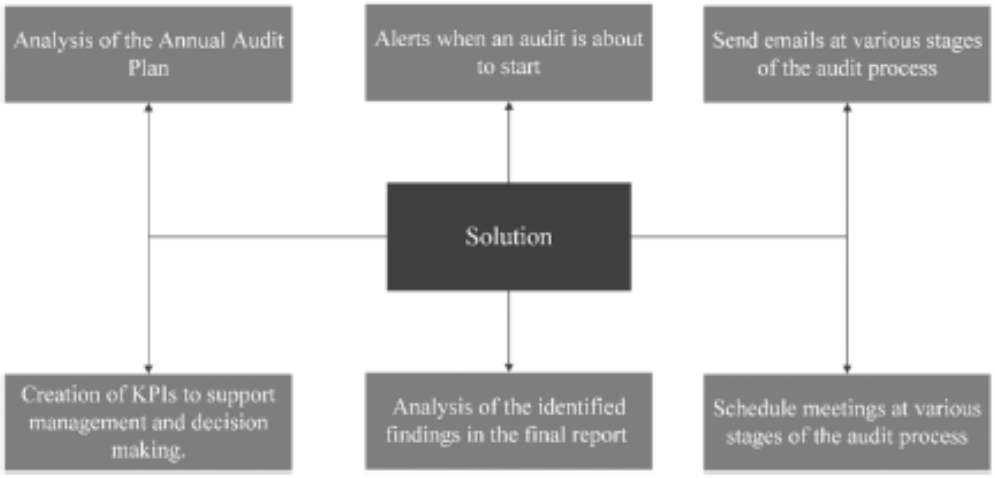


Fig. 2. Objectives of a solution.

Table 1
Top 5 best RPA tools (Adapted from (Software Testing Help, 2023)).

	Keysight's Eggplant	Blue Prism	UiPath	Automation Anywhere	Pega
Cost	Contact them for pricing.	$ 15,000 to$ 18,000 annually.	Free	Contact them for pricing details.	Start from $ 200/month
Maintenance and support services by the company	Documentation, Videos, FAQs, Tickets, etc.	Help Guide, Online-portal, Email, Contracts, & Training's	Training, Video tutorials, Community forum, & Implementation support	Training & Certifications	Training & Certifications, Community forum, Installation guide
Scalability	Extensible & can meet new challenges.	N/A	Can handle any process, in any number irrespective of its complexity	Yes. Scalable.	Scalable to Enterprise level.
User-friendliness	Process experts.	Yes. Developers	Yes. Even for non-developers	Yes. For anyone.	Yes. It supports low-code development.
Industry size	Small to large	MediumLarge	SmallMediumLarge	MediumLarge	MediumLarge

which include audit effectiveness, feedback on findings, audit duration and timeliness, and the value added by internal audit functions (Metricstream, 2023). These KPIs, such as the percentage of completed audits, number of planned audits, findings categorized by severity, and hours spent per audit, are vital for demonstrating the alignment of audit activities with management's expectations (AuditBoard, 2019). Power BI's intuitive interface allows for the creation of detailed dashboards that facilitate data-driven decision-making, thereby enhancing the analytical capabilities of the automation framework and ensuring that internal audit functions meet their objectives effectively.

3. Design and development

This section outlines the third step of the DSRM, which involves the creation and detailed description of the artifact's functionality. It breaks down the process into specific sections, each illustrating the steps taken and the main outcomes. A focus is also placed on the dependencies identified in the project, crucial for its execution.

4. Multivocal literature review

The Multivocal Literature Review (MLR) (Garousi et al., 2019) is similar to the Systematic Literature Review (SLR) (Garousi et al., 2016; Kitchenham and Charters, 2007) and aims to incorporate the so-called "grey literature" to supplement the published (formal) literature. MLRs are SLRs that include both scholarly writing (also known as academic writing or formal writing) and the (informal) grey literature (GL). Scholarly writing is the genre of writing used in all academic fields. GL is a multisource of information, which may exist in the form of blogs, videos, webpages, and white papers that are produced outside academic forums and are not subject to any quality control mechanism (e.g. the peer review process) before publication.

By including information that normally would not be considered due to its "grey" nature (Garousi et al., 2019), MLRs are important for the completeness of the research. An MLR in each subject field is essentially a combination of the sources that would be studied in an SLR and a Grey Literature Review (GLR) in the same field. Thus, an MLR is, in principle, expected to provide a more complete picture of the evidence in a given field. Figure 3 represents the relationship between SLR, GLR and MLR.

In the swiftly evolving domain of auditing, and IT, several researchers have recognized the value of incorporating GLR to enhance the comprehensiveness and applicability of their studies. This approach not only enriches the research by broadening the knowledge base but also ensures the credibility of the information remains uncompromised. Evidence of the successful integration of the MLR in the audit field can be found in several key studies referenced in (Van den Oever, 2020; Amaro et al., 2022; Pokhrel et al., 2020), and (Kamei et al., 2018). These studies confirm the practical utility of the MLR methodology, which we have adopted in our current research to draw upon a diverse array of knowledge sources. These sources provide various perspectives and

Fig. 3. The relationship between SLR, GLR and MLR.

objectives that are currently available, enriching the scope and depth of the audit literature (Ogawa and Malen, 1991).

In Table 2 of the study, we differentiate between "White" and "Grey" literature sources, where the aggregation of both forms the basis of the MLR. It is pertinent to note that to maintain the credibility of the data, literature including ideas, concepts, thoughts, and communications through social networks, tweets, and emails have been excluded (Garousi et al., 2019).

This MLR aims to identify and thoroughly examine the primary risk factors associated with the implementation of automated auditing tools, as reported by various auditing professionals. This involves exploring whether there exists a consensus among experts on the most effective strategies to mitigate these risks during implementation. The use of MLR allows the study to transcend the confines of conventional scientific literature by incorporating a wider spectrum of knowledge, thus enhancing the analysis process while maintaining rigorous quality standards (Garousi et al., 2019; Ogawa and Malen, 1991).

In the domain of auditing and the integration of RPA, the MLR process is depicted in Fig. 4 and unfolds in three phases. The initial phase of the research, titled "Planning the MLR," consists of two fundamental steps:

- Determining the necessity of conducting an MLR for auditing and RPA.
- Defining the objectives of the MLR and formulating specific research questions relevant to RPA in auditing.

While numerous guidelines exist for conducting an SLR, the MLR incorporates phases that diverge from traditional SLRs, particularly in the process of assessing the quality of information sources and their thorough investigation. Consequently, we will adapt the SLR guidelines to facilitate the execution of this MLR. As illustrated in Fig. 4, the structure of these guidelines for the MLR encompasses the planning, conducting, and reporting phases, as proposed by Garousi et al. (Garousi et al., 2019).

With the implementation of this model, it is anticipated that the inclusion of grey literature will furnish critical insights regarding the risks associated with implementing RPA in auditing processes. However, incorporating such literature introduces new challenges, primarily because it often relies on the practical experiences and opinions of professionals actively engaged in the field. To address these challenges and ensure robust data collection, this research will employ systematic guidelines to conduct the MLR (Garousi et al., 2016). This approach will allow for the application of specific inclusion and exclusion criteria, akin to those used in SLRs, to filter the results obtained through the world's leading search engine, Google. This methodology aims to provide a structured and comprehensive aggregation of both academic and grey literature, thereby enhancing the depth and applicability of the findings.

During the conducting review, the search string defined above was searched via Scopus, Web of Science, IEEE Xplore, ACM digital library, and Google - the last one for grey literature:

- (("robotic process automation" OR rpa OR "intelligent process automation") AND (audit*))

After acquiring potentially relevant primary sources, the following filters were established as illustrated at Table 3.

Regarding grey literature, Filter 2 undergoes modification; specifically, the Query Title is utilized instead of Query Abstracts. During the protocol definition stage of the MLR's planning phase, selection criteria were established to minimize the risk of bias. These criteria are articulated through inclusion and exclusion parameters, as detailed in Table 4.

The limitation associated with using Google Search, particularly regarding the replicability of searches at specific times, was acknowledged. Nonetheless, some scholars contend that methodologies for website searches can vary, emphasizing the importance of a well-thought-out rationale tailored to the specific goals and objectives of each review. This perspective suggests flexibility over adherence to a single methodological approach. Thus, careful planning and execution of the research, systematic screening of results, and the establishment of effective management structures are essential to ensure the robustness of this methodology (Stansfield et al., 2016).

Consequently, it is recommended to perform an extensive search of grey literature using at least one standard search engine (e.g., Google, Yahoo, or Bing) and to consider the first 12 pages of results instead of limiting the review to just the first 5 pages. Additionally, it is advisable to conduct a detailed examination of academic databases that are closely related to the research topic. This comprehensive approach ensures that all relevant literature, both grey and academic, is considered, thereby supporting the development of more thorough and substantive conclusions (Bellefontaine and Lee, 2014; Coleman et al., 2020).

The outcomes of the research are presented in Table 5, which lists a total of 61 documents: 18 white papers and 26 pieces of grey literature. The technique of snowballing yielded an additional 17 white papers, identified through references cited in our initial set of documents.

5. Audit

The term 'audit' originates from the Latin 'audire', meaning 'to listen', and aims to assure that financial statements are free of significant fraud or errors before reporting to stakeholders (Financial Reporting Council, 2023; Hayes et al., 2014). An audit evaluates a company's performance or systems, often lengthy when performed manually (Widuri et al., 2019). Typically, audits follow a four-stage pattern detailed in Table 6.

Regardless of the client's IT or accounting complexity, auditors are required to carry out audits within the criteria of the regulations. The client is likely undergoing processes involving advanced analytical techniques and new data sources. The increasing use of Big Data and the subsequent application of more advanced analytics by clients are the most recent challenges facing auditors (D. Appelbaum and Nehmer, 2017). That is why automation is so present in audits nowadays.

According to the research, there is no agreement on which activities should be automated. However, there is a requirement to automate highly structured and repetitive processes (Griffiths and Pretorius, 2021).

6. Robotic process automation

The results of the MLR examining the integration of RPA in audit practices yield compelling insights into its benefits. This review, encompassing a diversity of perspectives and sources, provides a nuanced understanding of how RPA can enhance audit procedures. The systematic analysis reveals advantages, from operational efficiencies to strategic enhancements, that RPA contributes to the audit process. Table 7 summarizes the benefits found, serving as a testament to the transformative impact of RPA on auditing.

As with any technological implementation, the adoption of RPA in

Table 2
Spectrum of the "White", "Grey" and Excluded literature (adapted from (Garousi et al., 2019)).

"White" literature	"Grey" literature	"Black" or other types of literature (excluded)
Papers published in journals.Conference ProceedingsBooks	Preprints; e-Prints; Lectures; Datasets; Gouvernement documents Standards; White papers; Technical reports; Blogs;Audio-video media	IdeasConceptsThoughts

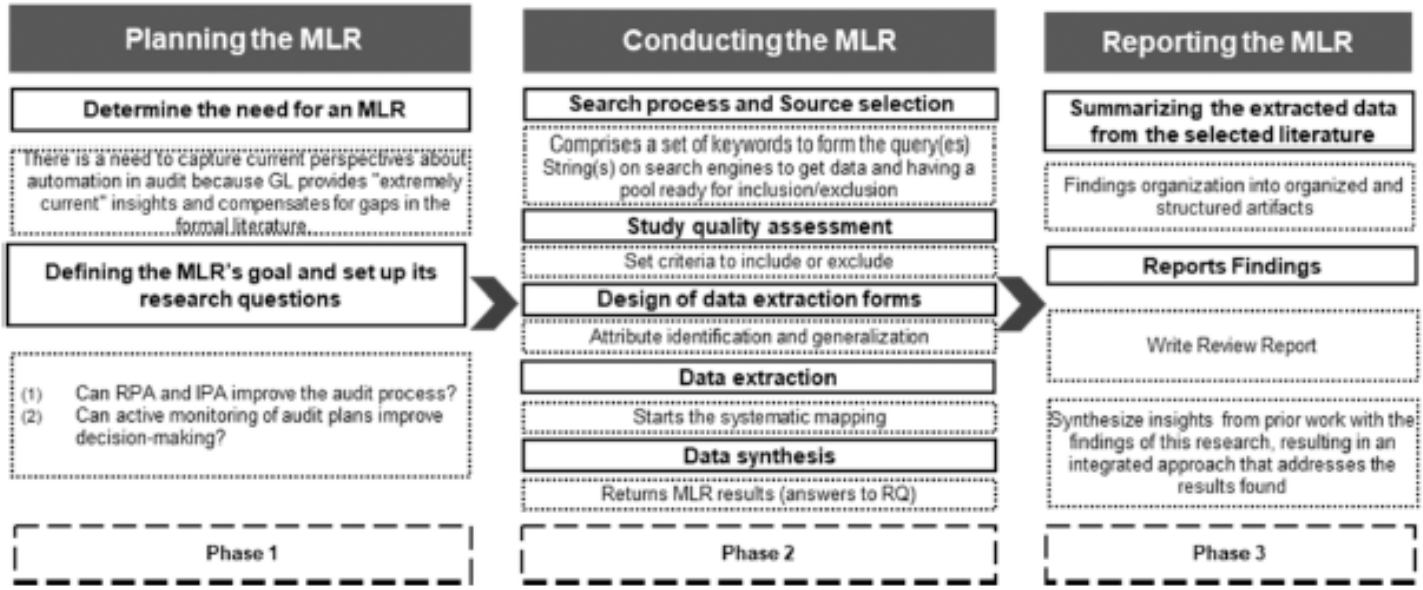


Fig. 4. Process stages for MLR: planning, conducting, reporting.

Table 3
Filters used in the literature review.

Filter 1	Query All Metadata, All documents
Filter 2	Query Abstracts, All documents
Filter 3	Relevant (inclusion/exclusion criteria)
Filter 4	Erase duplicates
Filter 5	Out of Scope
Filter 6	Snowballing

Table 4
Inclusion and Exclusion Criteria.

Inclusion Criteria	Exclusion Criteria
Written in English	Unidentified author
Since the 2000 s	Irrelevant topics such as medicine
Pdf's Document	Conference Review

Table 5
Review conclusions.

Database	Filter 1	Filter 2	Filter 3	Filter 4	Filter 5	Filter 6
IEEEXplore	25	16	16	3	2	+17
ACM Digital Library	437	2	2	2	2	
webofscience	100	30	30	0	0	
Scopus	3 329	104	61	55	14	
Google	16,500,000	479	41	26	26	
Total	**16,503,891**	**631**	**150**	**86**	**44**	**61**

auditing is accompanied by inherent risks that necessitate careful consideration. The outputs of the MLR offer not only a lens through which the benefits can be viewed but also shed light on the potential pitfalls and challenges. Table 8 distills the associated risks identified during the MLR, providing a comprehensive overview that auditors and decision-makers can reference to preemptively address and navigate these complexities.

RPA has implications for governance, control, and risk management in the organization. Before any RPA implementation, governance structures should be in place (Steinhoff et al., 2019). Concerns about privacy and security have an impact on the risk environment because the collection of digital evidence during auditing may expose sensitive (KPMG, 2018b; Mandal et al., 2017; Moffitt et al., 2018b; Syed et al., 2020b; Wojciechowska-Filipek, 2019b). To put it another way, the risk of organizational cybersecurity breaches may be on the rise.

These risk areas will require changes to the organization's risk assessment and may necessitate changes to auditing standards (D.

Table 6
Audit Processes (Adapted from (Chicago State University, 2023)).

Processes	Description
Planning	The auditor notifies the client of the audit, meets with organization management to discuss the scope and objectives of the examination, gets information on critical processes, analyzes current controls, and plans the remaining audit stages.
Fieldwork	Transaction testing and informal communication are the focus of the fieldwork. The auditor assesses whether the controls identified during the preliminary review are functioning effectively and, in the way, stated by the client during this phase. The fieldwork stage ends with a list of important findings from which the auditor will construct the audit report's final draft.
Audit Report	The final report, in which we document our audit findings and recommendations for improvement, is our main product. This also includes the response and implementation plan from management, as well as the completion timeline and responsible individual(s). Internal Audit discusses the rough draft with the client before issuing the final report to facilitate communication and guarantee that the recommendations written in the final report are practical.
Follow-up review	The client response documentation is examined, and the actions taken to address the audit report findings may be put to the test to ensure that the desired outcomes were achieved. In the follow-up report, all unresolved findings will be discussed.

Table 7
Benefits of RPA in Audit.

Benefits	References
Savings in human efforts	(Anagnoste, 2017; Gotthardt et al., 2020; Handoko et al., 2021b; Herrera et al., 2020; Mandal et al., 2017; Moffitt et al., 2018b)
Increased value-add talent	(Anagnoste, 2017; Handoko et al., 2021b; Herrera et al., 2020; Mandal et al., 2017; Moffitt et al., 2018b)
Increased agility for transformation	(Herrera et al., 2020)
Reduced errors	(Herrera et al., 2020; Moffitt et al., 2018b)
Increase in speed of delivery	(Handoko et al., 2021b; Herrera et al., 2020; Mandal et al., 2017)
Customer satisfaction/ advocacy	(Handoko et al., 2021b; Herrera et al., 2020; Mandal et al., 2017)

Table 8
Benefits of RPA in Audit.

Risks	References
Privacy and Security	(KPMG, 2018b; Mandal et al., 2017; Moffitt et al., 2018b; Syed et al., 2020b; Wojciechowska-Filipek, 2019b)
Compliance risks	(Deloitte, 2020; KPMG, 2018b; Mandal et al., 2017; The New Frontier Of Automation: Enterprise RPA, 2017)
Selecting the wrong tool	(Deloitte, 2020; Handoko et al., 2021b; KPMG, 2018b; Mandal et al., 2017; Moffitt et al., 2018b; The New Frontier Of Automation: Enterprise RPA, 2017)
Costly maintenance	(Deloitte, 2020; KPMG, 2018b)

Appelbaum and Nehmer, 2017). Controls that ensure the confidentiality, integrity, authenticity, and reliability of data used by RPA software should be implemented (Wojciechowska-Filipek, 2019b).

Opting for an inappropriate sourcing model may incur significant financial implications (Deloitte, 2020; Handoko et al., 2021b; KPMG, 2018b; Mandal et al., 2017; Moffitt et al., 2018b; The New Frontier Of Automation: Enterprise RPA, 2017). Such fiscal burdens often arise within organizations that elect to internalize all operations without the requisite expertise in governance, development, and implementation, or those that select inexperienced advisors or engage them after crucial decision-making junctures.

Conversely, the integration of Robotic Process Automation in the confidential information disclosure processes to banking authorities has demonstrated a decrement in the risk of non-compliance regarding information security and statutory mandates (Wojciechowska-Filipek, 2019b). RPA's reduction of procedural errors presents a potential solution to compliance-related challenges (Deloitte, 2020; KPMG, 2018b; Mandal et al., 2017; The New Frontier Of Automation: Enterprise RPA, 2017). It is incumbent upon organizations to meticulously assess the varied deployments of RPA to align with strategic objectives and mitigate business impacts (Hale et al., 2020). A comprehensive analysis of the associated risks of adopting RPA and Intelligent Process Automation within the audit function is presented in Table 9.

7. Solution design

The project utilized UiPath Studio Community, selecting appropriate project types and templates which influenced the dependencies in the Studio. Key dependencies integrated into the project include *UiPath.DocumentUnderstanding.ML.Activities* for machine learning features in document processing, *UiPath.PDF.Activities* for comprehensive document management, *UiPath.Mail.Activities* for email operations, *UiPath-Team.OutlookCalendar.Activities* for managing Outlook calendar events, and *UiPath.Excel.Activities* for handling Excel operations. These dependencies were critical in enabling functionalities like machine learning-based document reading, email handling, and meeting scheduling, highlighting UiPath's capacity to facilitate complex tasks with minimal development expertise. The subsequent sections will delve into the development stages of the solution.

Table 9
Identified targeted risk categories for implementing a program with RPA and AI (Adapted) (Mandal et al., 2017).

Business Risks		Automation Risks	
Executive	Who designs control systems?Who will manage the framework and promote efficiencies?	License Compliance; Automation strategy and governance.	Proof of Concept
Functional	Who designs control systems?Are any scalability limitations in RPA and core systems?	Adapting schemes of existing systems with new features;Legacy systems for simultaneous and unified operations across technical testing and rollout.	Backward Compatibility
Technical	How will the data quality and accuracy be ensured?	Incident management and business continuity;Regulatory compliance.	Implementation
Operational	Which controls need to exist to monitor performance?How will the business comply with regulatory requirements?	Data leakage and privacy;Cyber threats.	Business Case

8. Annual internal audit plan

The annual internal audit plan serves as a key document outlining the audit engagements scheduled for the upcoming year, tailored to the specific needs of each organization (AuditNet, 2023). Initially, defining essential attributes for the audit plan is critical, as these characteristics form the basis of the development process and are instrumental in automating routine tasks such as email correspondence. Key elements include the email addresses of the auditor and the auditee, the audit's name, and the start date, all crucial for operational effectiveness. A thorough review of existing audit plans from public entities ensures alignment with these criteria, although some plans may show structural inconsistencies such as poorly formatted tables or imprecisely noted dates. Effective collaboration between development and business teams is essential to address any potential modifications that might impact the development process. This collaborative approach aids in maintaining a robust audit plan that supports automated functions like scheduling and sending alerts for upcoming audits, thereby enhancing the efficiency and accuracy of the internal audit function.

9. Launching the audit process

In the second stage of the audit initiation process, the automation system plays a pivotal role. Upon determining which new audit is about to start, the robot begins by creating the necessary organizational structure. This involves setting up designated folders for different phases of the audit, specifically for communication, execution, and reporting, at a URL specified by the auditor.

Following the creation of these folders, the RPA then proceeds to facilitate initial communications. It sends an email to notify involved parties of the upcoming meeting and schedules this meeting based on the date previously provided by the auditor during the initial planning phase. The communication email, as illustrated in Fig. 5, leverages data pulled from the audit plan, including the audit name, scope, the email of the audited area, and the auditor's email. Post this communication, the robot does not engage further, leaving any potential meeting cancellations or rescheduling to be handled directly by the auditor.

Subsequently, the RPA verifies the existence of an information request list, an essential artifact for the collection of audit evidence. Acknowledging that this document may not be readily accessible, the system is configured to conduct daily searches for up to five days. Should the document remain undiscovered after this interval, the robot dispatches an email notification to the auditor, indicating the necessity for manual intervention in the document transmission process. Conversely, if the document is located within the prescribed period, the robot immediately forwards it to the auditee, as illustrated in Fig. 6.

This automation of evidence requests and communication significantly streamlines the auditing process, making it more efficient by reducing delays and manual intervention. These steps, along with the entire audit plan analysis process, are summarized in the Information Flowchart shown in Fig. 7. This flowchart provides a visual overview of the sequence and interactions of the tasks involved in this audit initiation stage.

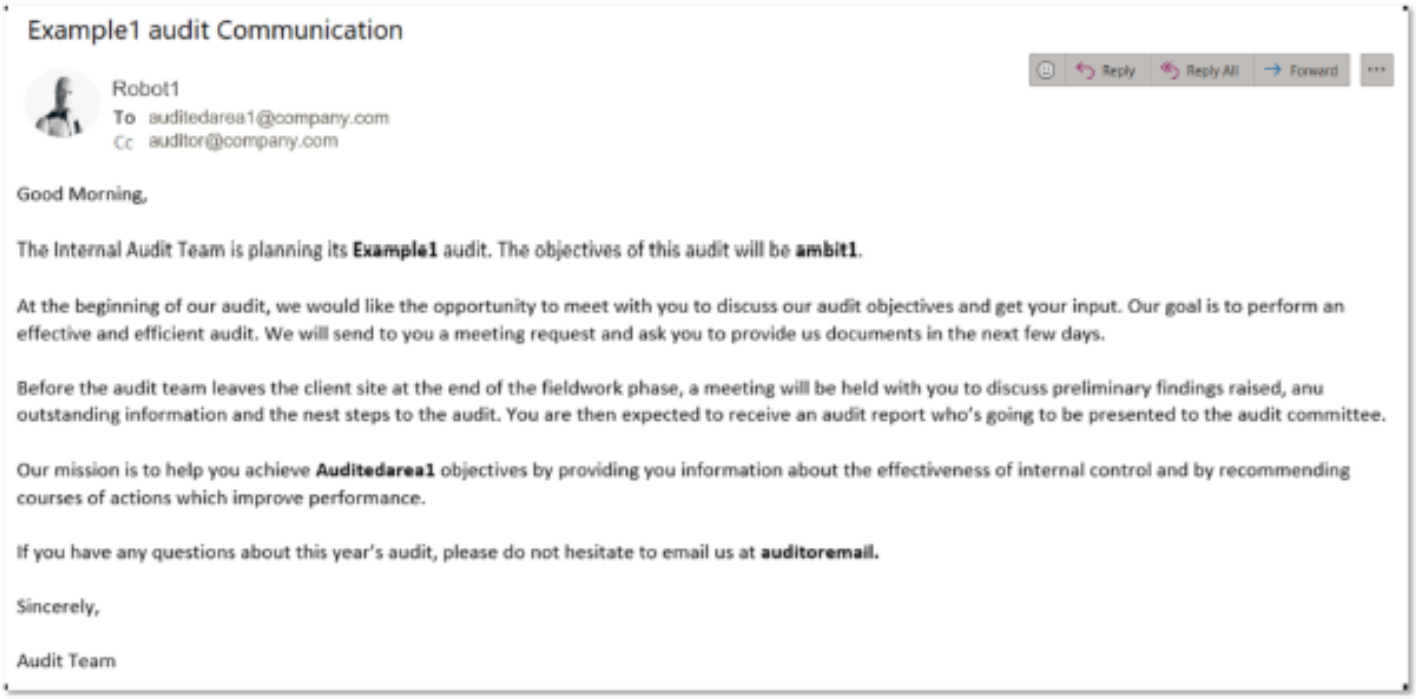


Fig. 5. Communication email output.

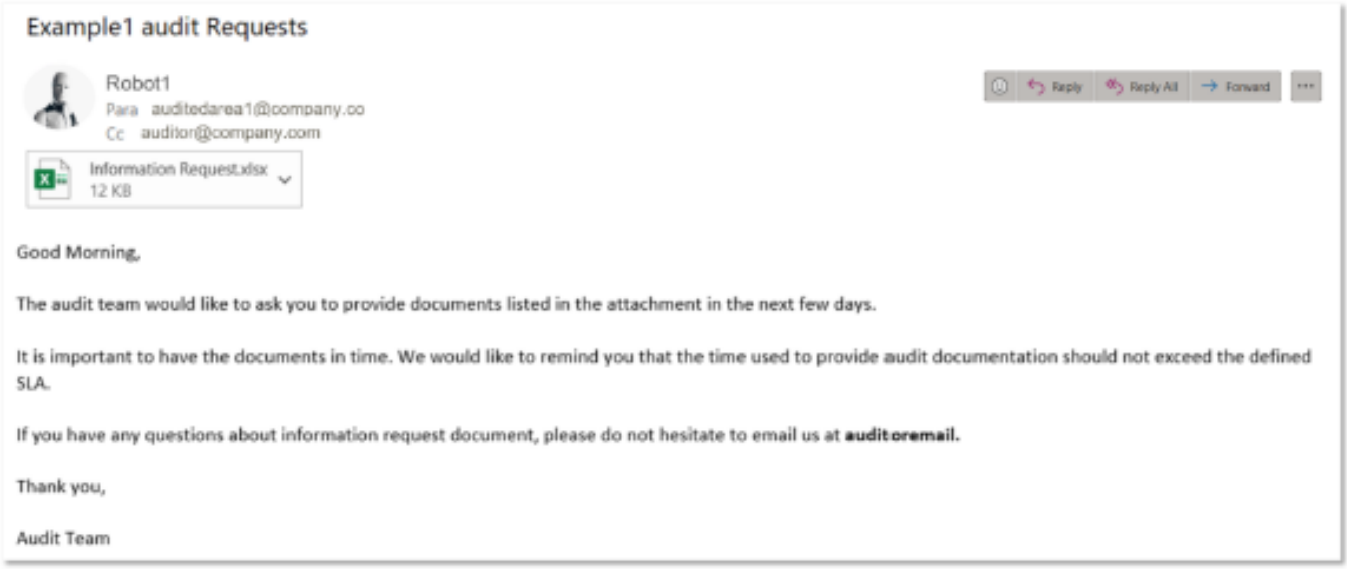


Fig. 6. Information request email output.

9.1. Reporting tool

The third phase of the audit process culminates in scheduling the final meeting and dispatching the final report, following a 15-day period allocated for fieldwork. This duration may be adjusted depending on the actual time spent in fieldwork. Should the final document not be present in the designated folder after this period, the robotic system initiates daily checks for up to five days. Failure to locate the document prompts the robot to notify the auditor to take over the document-sending phase. Conversely, if the document is located, the robot seeks the auditor's approval to send it and to schedule the final meeting, requesting the meeting date in the format dd/MM/yyyy. Approval from the auditor triggers the robot to execute these tasks. The format for the final report email is derived from a template used by The University of Texas at Dallas, as illustrated in Fig. 8. This automated process ensures efficiency and timeliness in the final stages of the audit.

The robot then moves on to the activity where it reads the report and takes the information from the findings table, with the CV technique's help. The CV activities used for reading the audit plan are used again for analyzing the final audit report. However, as the final audit report is usually a longer document, additional steps had to be added to ensure that the table summarizing the findings status is read.

To ensure the robot locates the required table, the Send HotKey activity is used following the CV Screen Scope activity to perform a page down if the "Finding Status" table isn't initially found. This part of the process, which involves the robot methodically reading each screen element, may take a few seconds.

Additionally, a final audit report template closely mirroring real-world business formats is utilized, sourced from The Internal Auditor's website, which offers resources to enhance audit effectiveness (The Internal Auditor, 2023). Table 10 in the final report displays this "Finding Status" table, showcasing the practical application of these templates.

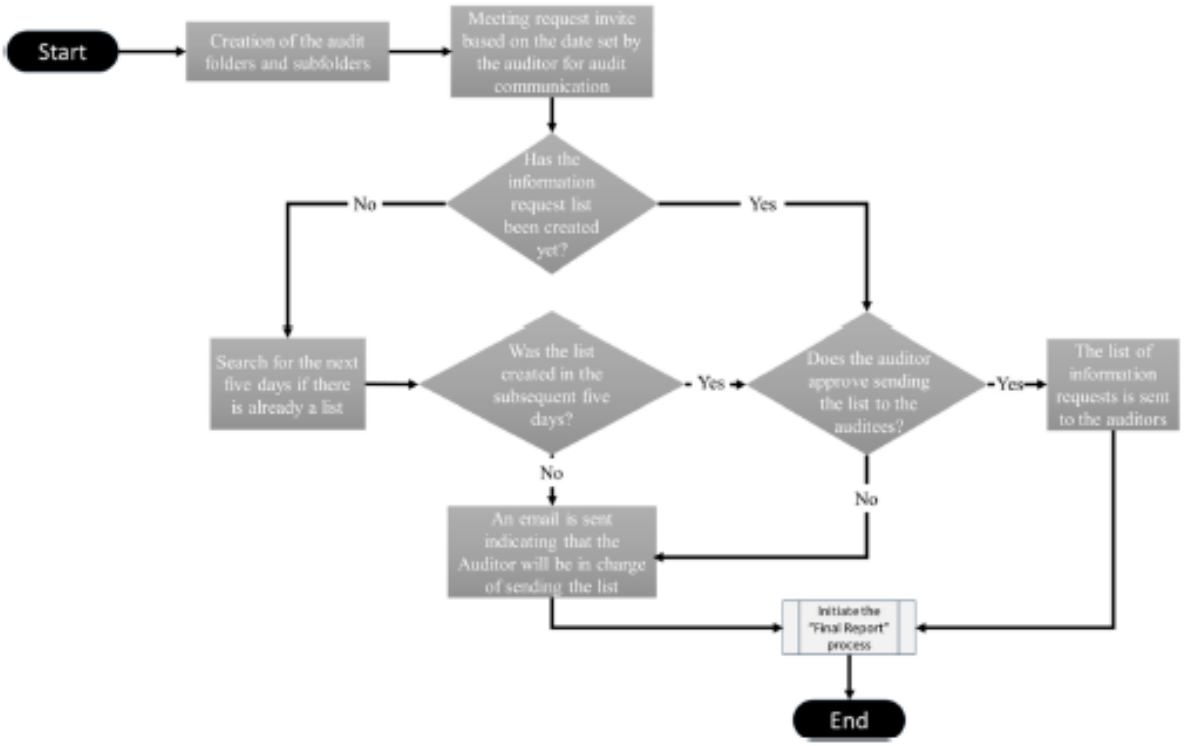


Fig. 7. Information flowchart.

Fig. 8. Output Final Report email (Adapted) (Stephen S., 2020).

Table 10
Findings Status (example).

Findings Status	Critical	Significant	Less Significant	Minor	Total
Number of Findings	0	4	1	5	10
Cleared Findings	0	0	0	0	0
Findings to clear	0	4	1	5	10

Upon completion of the table reading process via the Computer Vision (CV) activity, the Write Range activity is employed to transfer the data table, which contains the finding status table, to another Excel file. It is noteworthy that this step is undertaken exclusively when the document is in PDF format.

Following the extraction of the table into an Excel sheet, the robot concludes its role in this development phase. These final activities, along with the entire process of analyzing the audit plan, are succinctly summarized in Fig. 9.

It should be noted that at both the commencement and conclusion of the development, two variables are designated to record the actual start and end dates of the audit. These variables are subsequently extracted to an Excel file to calculate KPIs, a topic that will be elaborated upon in the following section.

10. Key performance indicators

As noted earlier, Power BI will be employed to integrate data from

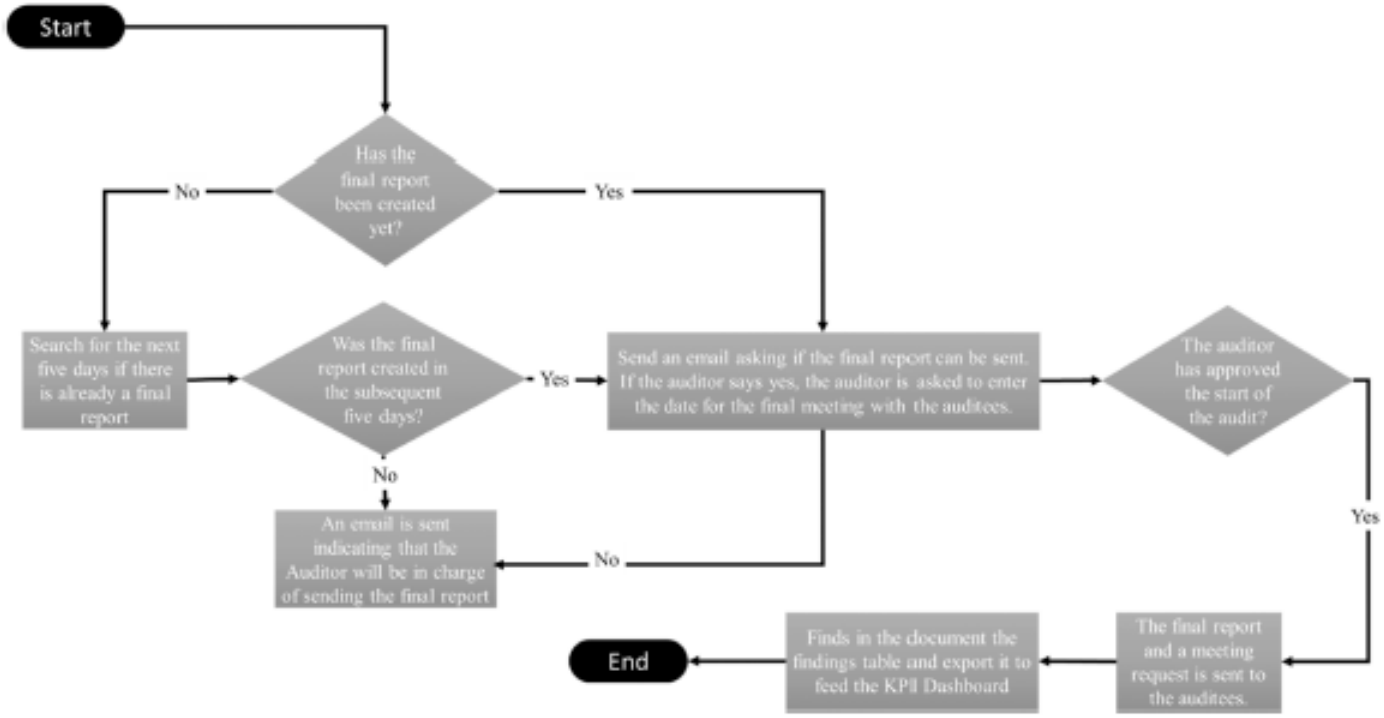


Fig. 9. Final Report Flowchart.

IPA databases to facilitate precise, data-driven audit decisions and illustrate how audit activities align with the strategic objectives of the company (Lu and Chesbrough, 2021). The KPIs commonly used include (AuditBoard, 2019):

1. Percentage of completed audits;
2. Count of planned audits;
3. Count of findings found per gravity; and
4. Hours spent per audit;

Correspondingly, three Excel workbooks have been developed during the IPA process containing data tables for (1) the audit plan, (2) the finding status of completed audits, and (3) the actual start and end dates of the audits. These workbooks will be integrated into the Power BI dashboard to enhance the visual representation of the data. This integration is depicted in Fig. 10.

A comprehensive visualization was developed using the Power BI tool, incorporating all identified KPIs into a single-page report for a managerial overview. The report features both iterative and informative visual elements, employing the Zebra BI matrix visual - a highly effective Power BI table that enables the creation of detailed and visually appealing reports (Zebra BI, 2023). This tool allows for dynamic filtering of data by auditor, audited department or area, and year, providing a segmented analysis of each KPI. Additionally, it supports the comparison of current findings with previous audits and checks if the actual time spent on an audit aligns with the estimated time. The report, in Fig. 11, is designed to be user-friendly and continuously updated, aiding management in evaluating audits, managing team performance, and informing decisions related to resource allocation, future audit planning, and scope improvements. This ensures that management decisions are well-supported by timely and relevant data insights.

In conclusion, the final stage is critical as it allows management to evaluate real data without human interference, identifying audits that may need more time or have issues. This data-driven insight helps in making informed decisions about enhancing the IPA system, ensuring effective reporting to the board while preventing unnecessary expenditures and automation failures.

11. Demonstration and evaluation

This section aims to demonstrate step four of the DSRM which is to demonstrate that the artifact is effective in solving the problem. To respond to this important step, some auditors from the banking sector in Portugal were asked to give their opinions about the implemented

Fig. 10. Data bases scheme.

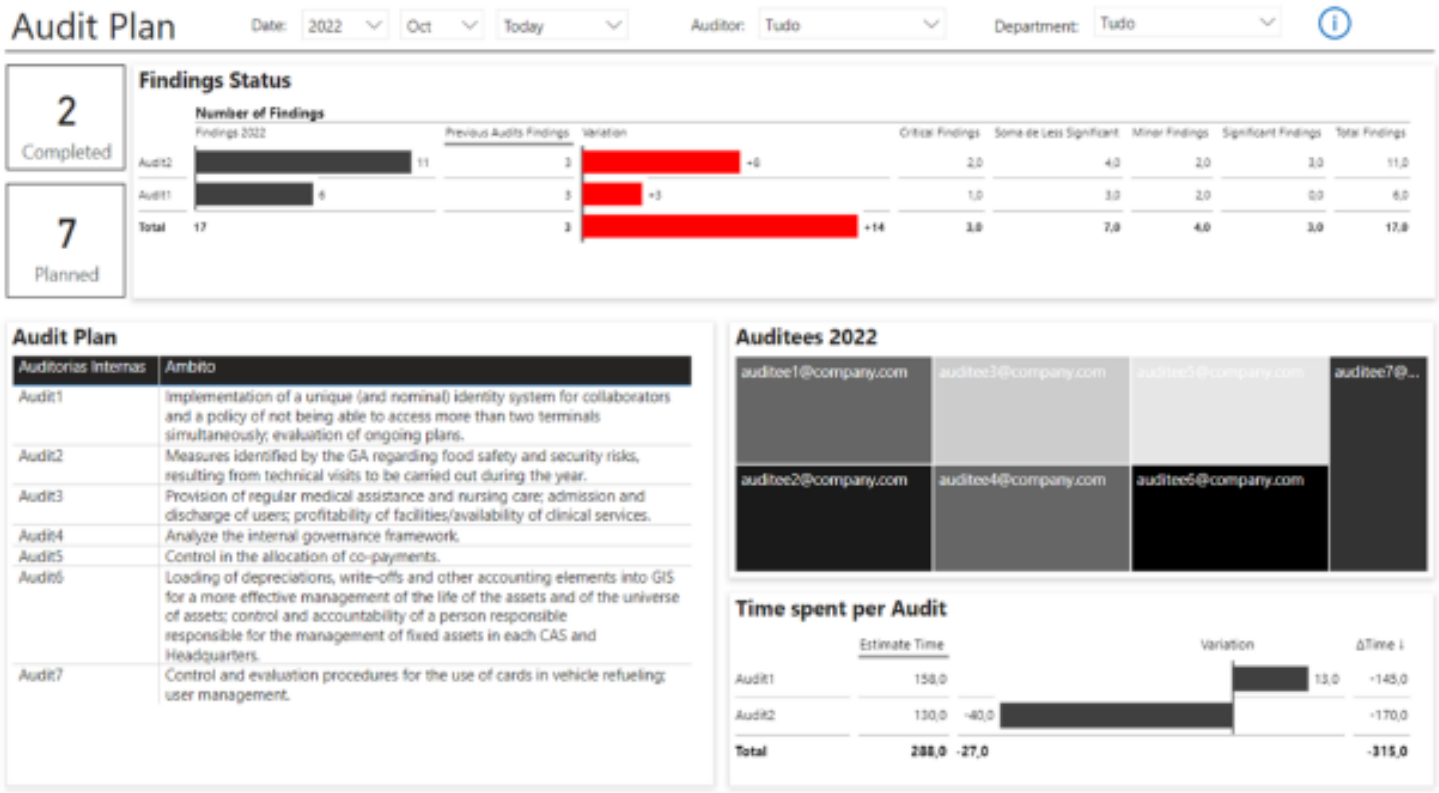


Fig. 11. Power BI dashboard.

solution. The response from auditors turns out to be one of the most important in understanding the need for the solution developed in this area since they are the ones facing the changes in the process with the implementation of IPA.

To evaluate the proposed artifact, numerous interviews were conducted with experts and professionals from both fields. Interviews are a fundamental component in social science research, extensively discussed in various publications on research methodology (Eisenhardt, 1989; Hollweck, 2015). The objective of these interviews is to draw inferences about a broader population by analyzing a sample from that population. This approach stands in contrast to a census, which seeks to gather observations from the entire population and is another method employed for evaluating artifacts. Consequently, for this study, a semi-structured questionnaire was utilized to assess the proposed artifact.

In this study, the artifact underwent evaluation based on its construct and model using specific principles. These included completeness, ease of use, fidelity to real-world phenomena, internal consistency, level of detail, simplicity, understandability, importance, accessibility, and suitability, as delineated by March and Smith (March and Smith, 1995) and Rosemann and Vessey (Rosemann and Vessey, 2008). Guided by these principles, a semi-structured questionnaire was developed, as detailed in Table 11.

As emphasized earlier, assessment is crucial within the DSRM. To evaluate the artifact effectively, professionals from both the BC and Audit sectors were selected, who possessed various levels of experience and expertise. This approach was intended to deepen the rigor of the evaluation and ensure the artifact's practical applicability.

Table 11
Semi-structured questionnaire for evaluation of the purposed artifact.

	Criterion	Statement
1	Completeness	The introduction of automation into the audit process contains all the rules and standards of both realms.
2	Ease of use	The introduction of automation into the audit process is well-described and easy to verify and implement in both contexts.
3	Fidelity with real-world phenomena	The proposed artifact corresponds to possible solutions.
4	Internal consistency	The findings to introduce automation into the audit process use adequate terminology, are well-written, and are justified by the theory.
5	Level of Detail	The proposed artifact contains a sufficient level of detail in each mechanism for each area.
6	Simplicity	The proposed artifact contains the necessary practices and it is easy to implement.
7	Understandability	The proposed artifact is easily understood as a good practice for both BC and Audit practitioners.
8	Importance	The proposed artifact is important for both practitioners and academics.
9	Accessibility	The proposed artifact has an understandable terminology with a practical perspective, not only a theoretical one.
10	Suitability	The proposed artifact of practices is applicable in the practice of both realms.

12. Interview questions

To gather conclusive data, it was essential to ask respondents the right questions, covering basics like age, gender, and professional background, as well as their experience with automation. Initial questions gauged auditors' awareness and perceptions of automated processes in their company and their impact on management. Subsequent inquiries sought evaluations of specific automated activities, such as alerting auditors of upcoming audits, scheduling meetings, sending informational emails, and generating a Power BI report to support KPIs. Auditors rated the value of these automations on a scale from 0 (not useful) to 5 (very useful). Finally, two optional open-ended questions were posed to collect feedback on desired automation and potential improvements in the development process.

13. Population and sample

The population under consideration comprises auditors from four Portuguese banks and offers insightful details about the composition of audit teams in terms of qualifications, age, roles, and gender. Table 12 provides an overview of the characteristics of the sampled population for the study.

Educational background:

A majority of the auditors (53%) hold bachelor's degrees, indicating that this level of education is sufficient for most auditing roles within these banks.

The significant portion (42%) with master's degrees suggests a high level of expertise and possibly a preference or requirement for higher education in more complex audit functions.

Only a small fraction (5%) has post-graduate qualifications, reflecting perhaps that such advanced degrees are not typically necessary for the roles filled by the respondents.

Age Distribution:

Nearly half (47%) of the auditors are between thirty and thirty-nine years old, suggesting a mature workforce with substantial professional experience.

The representation across other age groups (23% between forty and forty-nine, 18% younger than twenty-nine, and 12% over fifty) shows a broad range of ages, which can contribute to diversity in perspective and approach within the audit teams.

Roles within Audit Departments:

The vast majority (82%) being technicians indicates that the primary need within these audit departments is for hands-on auditing work.

The presence of coordinators (12%) and directors (6%) suggests a structured hierarchy but with relatively few in leadership roles, emphasizing a pyramid structure in staffing.

Gender Distribution:

The gender split shows a slight male predominance (58%) but is relatively balanced (42% female), suggesting no significant gender disparity. This balance may contribute to diverse viewpoints and approaches to auditing, potentially enhancing the effectiveness and comprehensiveness of audits.

Overall, the survey highlights a well-educated, age-diverse audit workforce with a reasonable gender balance, primarily composed of technical staff with a structured, yet minimal, leadership hierarchy. This composition could be indicative of a robust and dynamic auditing environment, capable of addressing various challenges and complexities within the banking sector.

In the context of determining the requisite number of interviews for qualitative research, Myers (2013) contends that the quantity is indeterminate and varies depending on the research question and the nature of the insights sought. The concept of saturation is achieved when no additional insights are garnered that contribute to the understanding of the research question (Myers, 2013; Myers and Newman, 2007). In the current study, which aims to evaluate and refine a model designed to streamline the audit process, saturation was attained after the tenth interview. Subsequent interviews, ranging from the eleventh to the seventh, did not yield any new insights that further elaborated on the proposed model as a possible solution.

Table 12
Profile of Auditors in Portuguese Banks: Qualifications, Age, Roles, and Gender Distribution.

Description	Details
Number of Auditors Surveyed	17
Banks Involved	4 Portuguese Banks (2 Large, 2 Small to Medium-sized)
Academic Qualifications	Bachelor's: 53% Master's: 42% Post-graduate: 5%
Age Distribution	<29 years: 18% 30–39 years: 47% 40–49 years: 23% >50 years: 12%
Job Roles	Technicians: 82% Coordinators: 12% Directors: 6%
Gender Distribution	Male: 58% Female: 42%

14. Data collection

In Table 13 below, we summarize the key findings from a recent survey conducted among auditors across four Portuguese banks. This table presents the auditors' responses to various aspects of automation within their audit processes, illustrating their levels of awareness, acceptance, and resistance to automated activities. The responses are categorized into several key areas of automation implementation and evaluate their impact on the audit workflow. This data aids in understanding the current stance of audit professionals towards automation and highlights areas where further discussion or intervention may be necessary.

The survey results among auditors in Portuguese banks generally show a positive attitude towards automation in audit processes. A significant majority of auditors are aware of and acknowledge the benefits of automation, with nearly unanimous support for an automated alert system and strong approval for Power BI reporting.

However, some resistance remains, notably with routine task automation like email notifications, where about 12% expressed disagreement. This resistance could stem from concerns over job security or the adequacy of automation for complex tasks.

Responses also indicate that perceptions of automation's benefits may vary by role, with less direct involvement leading to more neutral views. Despite some resistance, the overall acceptance suggests a favorable outlook for further integrating automation into audit practices, though continued education and dialogue will be crucial to address lingering doubts and ensure widespread adoption.

15. Discussion

This section critically examines the findings of the study, integrating both theoretical insights and practical implications of deploying IPA within the auditing processes of financial institutions, particularly in the banking sector. While the integration of IPA offers significant enhancements in efficiency and strategic decision-making, it also presents

Table 13
Auditor attitudes towards automation in audit processes.

Survey Aspect	Response	Comments
Awareness of Automated Activities	94% aware	
Resistance to automation	18% reported resistance	Some auditors showed doubts or resistance.
Impact of Automation	88% positive impact	
Support for Audit Alert System	100% support	65% totally agree.
Approval of Automatic Email Notifications	82.35% agree	11.77% disagreed, 5.88% neutral.
Scheduling and Sending of Final Report	58% approval	23.53% neutral, mostly technicians.
Scheduling Audit Communication Meetings	62.5% agree	
Implementation of Power BI Reporting	94% agree	1 neutral auditor identified resistance in audit areas.
Overall Rating of Solution (Scale 0–5)	94% rated above 4	Indicates a positive evaluation despite initial resistance to change.

challenges and raises important considerations for implementation and future development (Gegenhuber and Mair, 2024; Peñarroya-Farell and Miralles, 2021; Yun et al., 2022). Here, we discuss the broader implications of our findings, focusing on their relevance to banking sector policymakers, and delineating the theoretical contributions to the existing literature on business continuity and audit practices (Harsanto et al., 2022). This discussion aims to bridge the observed gaps identified in previous sections and suggests pathways for leveraging IPA to enhance audit effectiveness and organizational resilience. Moreover, it offers recommendations tailored to policymakers and industry leaders who are positioned to influence the adoption and regulation of emerging technologies within the audit domain (Bigliardi et al., 2020).

The integration of IPA within business continuity auditing, as explored in this study, has demonstrated substantial potential to streamline audit processes through the automation of routine tasks such as communications, information requests, and final report submissions. This shift not only enhances operational efficiency but also supports auditors in their critical role during technological transformations.

From a theoretical standpoint, this study contributes to the body of knowledge by bridging the gap between business continuity practices and the application of IPA in the auditing domain. It challenges existing theories that view automation merely as a tool for operational efficiency, proposing instead that automation is pivotal in enhancing the strategic decision-making process within financial institutions. This perspective suggests a paradigm shift where automation is seen as a transformative force that aligns closely with business goals rather than just a means to reduce labor costs.

Practically, the findings from this research have direct implications for banking sector policymakers:

- **Enhanced Compliance and Risk Management:** Automated tools can provide real-time data analysis, which is crucial for maintaining compliance with evolving regulations and managing risks proactively.
- **Strategic Resource Allocation:** By automating routine and time-consuming tasks, resources can be redirected toward more critical analytical and strategic functions. This not only improves productivity but also enhances job satisfaction among audit professionals by reducing monotonous tasks.
- **Decision Support:** With automation, audit data can be processed and presented in ways that support strategic decisions, providing insights that were previously difficult to extract manually.

The adoption of IPA in auditing represents a transformative opportunity for the banking sector. However, the successful integration of these technologies necessitates supportive policy frameworks and strategic initiatives from regulators and government bodies. These suggestions aim to maximize the benefits while mitigating potential risks associated with IPA, ensuring that the banking sector remains robust, compliant, and competitive in a rapidly evolving digital landscape:

- **Adopting Progressive Regulatory Frameworks**: Policymakers should consider creating and adapting regulatory frameworks that encourage the adoption of automation while ensuring robust data security and privacy standards.
- **Encouraging Investment in New Technologies**: There should be a clear directive from regulators and government bodies encouraging banks to invest in new technologies that facilitate transparency and efficiency in auditing processes.
- **Training and Development**: To overcome resistance to new technologies, comprehensive training programs should be implemented to ensure that the workforce is well-prepared to leverage these new tools effectively.

While the study effectively demonstrates the benefits of IPA in auditing, there remains a lack of discussion on:

- **Integration Challenges:** How do existing systems integrate with new automated tools without disrupting current operations?
- **Long-term Sustainability:** What are the long-term impacts of automation on employment within the banking sector, and how can these be mitigated?
- **Customization and Scalability:** How can these automated solutions be customized to fit different sizes and types of banks or financial institutions?

16. Conclusions

This study aimed to integrate automation within the audit process, thereby streamlining manual and repetitive tasks to enhance the efficacy of business continuity management. This goal was pursued through the identification of optimal automation solutions and the mitigation of associated risks.

A multi-stage methodological approach was utilized, beginning with an extensive literature review to identify the risks, benefits, and challenges linked with the automation of audit processes. This was followed by the application of the DSRM to precisely define the core problem and develop an appropriate solution. Subsequent phases involved the detailed design and development of the proposed solution, culminating in a survey conducted among bank auditors to evaluate how well the solution met their needs.

The findings from this study highlight the pivotal role of IPA in the audit process. Significant advantages were observed, including the implementation of an alert system that notifies auditors of upcoming audits and the use of KPIs to provide a detailed overview of the progress within the audit plan. These tools help identify areas that require refinement in audit management.

The integration of automated tasks, such as email correspondence and meeting scheduling, is expected to reduce the workload of auditors, increase operational agility, and accelerate the delivery of audit outcomes. This paper contributes a novel perspective to the auditing field, particularly in evaluating IT sectors, emphasizing the need to revolutionize auditing practices to allow auditors to focus on more critical tasks. Moreover, the significant reliance on non-peer-reviewed literature highlights the necessity for thorough academic scrutiny of the advancements in implementing technologies like IPA to strengthen business continuity management.

17. Limitations

While analyzing the survey results, a notable limitation emerged related to the diversity of the sample, which comprised four distinct companies varying in size from small to large banks. This variation introduced disparate realities into the data, as large firms often require more extensive automation due to the volume and repetitiveness of their processes. Conversely, smaller companies are typically more conservative in adopting automation strategies, largely due to budget constraints.

This disparity suggests that the solution discussed is optimally suited for larger organizations that manage comprehensive audit plans. Although characterized as low-cost, the implementation of this IPA solution still demands significant resources for continuous evaluation and adaptation to ensure its effectiveness across diverse organizational contexts. This observation underscores the need for tailored approaches in the automation of audit processes to accommodate the specific operational and financial contexts of different-sized institutions.

18. Future work

This study aims to inspire further enhancements in automated audit processes. Auditing plays a critical role in identifying risks and inefficiencies within organizational processes, necessitating the elimination of repetitive tasks. This research has shown the potential for increased agility in audit functions through comprehensive automation.

Although some activities are already automated during fieldwork, it remains essential to evaluate whether automation solutions are effective or merely resource-intensive.

The solution proposed operates continuously and can be implemented in audit departments at a minimal cost. It is also adaptable, allowing customization to meet specific organizational needs. Using KPIs to identify critical gaps (for instance, in annual audits that are time-intensive), helps management to strategically decide on expanding automation across the audit process.

Future initiatives should focus on integrating advanced modules within the existing development framework to cater to specific corporate needs. Feedback from this study has highlighted several potential enhancements. There was significant support for implementing automated alert systems at key stages of the audit process to monitor both the actual and projected timelines, as well as to provide timely updates on the remaining steps. There is also a demand for increased automation in tasks such as data extraction, procedural mapping, characterization of findings, and the regular dissemination of progress reports. These improvements aim to refine the automation process further, enhancing efficiency and effectiveness in audit operations.

Funding acknowledgement

This research received financial support from COPELABS (Grant Number: UIDB/04111/2020) for the preparation and submission of the article. COPELABS was not involved in the study design, data collection, analysis, interpretation, writing of the report, or the decision to submit the article for publication. The authors retained full independence in the research process and preparation of this manuscript.

CRediT authorship contribution statement

Ruben Filipe Pereira: Writing – review & editing, Supervision. **Micaela Freitas da Fonseca:** Visualization, Investigation. **José Cascais Brás:** Writing – review & editing, Writing – original draft, Software, Methodology, Data curation, Conceptualization. **Isalas Scalabrin Bianchi:** Writing – review & editing. **Rui Ribeiro:** Validation, Software, Resources.

Declaration of Generative AI and AI-assisted technologies in the writing process

In the preparation of this manuscript, generative AI and AI-assisted technologies were utilized only to enhance the readability and language quality. These technologies were applied under strict human oversight and control. The authors thoroughly reviewed and edited the outputs to ensure accuracy and reliability. Following Elsevier's AI policy, the AI was not listed as an author or co-author, and the responsibility for the manuscript's content lies solely with the human authors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Agoglia, C.P., Brazel, J.F., Hatfield, R.C., Jackson, S.B., 2010. How doaudit workpaper reviewers cope with the conflicting pressures of detecting misstatements and balancing client workloads? Auditing 29, 27–43. https://doi.org/10.2308/aud.2010.29.2.27.

Aksoy, T., Hacioglu, U.Auditing Ecosystem and Strategic Accounting in the Digital Era. 2021.

Alles, M.G., Kogan, A.Audit Automation for Implementing Continuous Auditing: Principles and Problems Audit 4.0 View project Applications of Data Analytics: Visualization and Cluster Analysis of Governmental Data View project. 2008.

Amaro, R.M.D., Pereira, R., Mira da Silva, M., 2022. Capabilities and practices in DevOps: a multivocal literature review. IEEE Trans. Softw. Eng. 1–24. https://doi.org/10.1109/TSE.2022.3166626.

Anagnoste, S., 2017. Robotic automation process - the next major revolution in terms of back office operations improvement. Proc. Int. Conf. Bus. Excell. 11, 676–686. https://doi.org/10.1515/picbe-2017-0072.

Appelbaum, D., Nehmer, R., 2017. The coming disruption of drones. Robots, Bots.

AuditBoardKPI Audit Checklist: Top Metrics to Track. Https://WwwAuditboardCom/Blog/Top-Metrics-to-Track-in-Your-Audits-Checklist/ 2019.

AUDITBOARD, 2018. What Is Robotic Process Automation? Can It Assist Internal Audit? |. AuditBoard. In: (https://www.auditboard.com/blog/5-ways-robotics-process-automation-can-assist-internal-audit/) (accessed June 19, 2023).

AuditNet. Annual Internal Audit Planning 2023. https://www.auditnet.org/audit-library/annual-audit-planning (accessed October 7, 2023)..

Bedard, J.C., Ettredge, M.L., Johnstone, K.M., 2006. Using electronic audit workpaper systems in audit practice: task analysis, learning, and resistance. SSRN Electron. J. https://doi.org/10.2139/SSRN.934201.

Bellefontaine, S.P., Lee, C.M., 2014. Between black and white: examining grey literature in meta-analyses of psychological research. J. Child Fam. Stud. 23, 1378–1388. https://doi.org/10.1007/s10826-013-9795-1.

Bharadhwaj, H., 2021. Auditing robot learning for safety and compliance during deployment. Blue Sky Pap. 5th Conf. Robot Learn. (CoRL 2021), Lond., UK.

Bigliardi, B., Ferraro, G., Vergata, T., Filippelli, S., Galati, F.The past, present and future of open innovation 2020. https://doi.org/10.1108/EJIM-10-2019-0296.

Brás, José, Guerreiro, S.Challenges for Assessing and Designing Business Continuity Processes 2016.

Brás, J., Pereira, R., Moro, S., 2023. Intelligent process automation and business continuity: areas for future research, 2023;14:122 Information Vol 14, 122. https://doi.org/10.3390/INFO14020122.

Brás, J.C., Pereira, R.F., Moro, S., Bianchi, I.S., Ribeiro, R., 2023. Understanding how Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755: 2020 and ISO/22301:2019. IEEE Access 1-1. https://doi.org/10.1109/ACCESS.2023.3337159.

Chambers, B.R.How Internal Audit Can Help You Sleep Better 2020;2:17–20.

Chicago State UniversityAudit Process | The Internal Audit Process from Beginning to End 2023. https://www.csu.edu/internalaudit/auditprocess.htm (accessed April 28, 2024).

Coleman, S., Wright, J.M., Nixon, J., Schoonhoven, L., Twiddy, M., Greenhalgh, J., 2020. Searching for programme theories for a realist evaluation: a case study comparing an academic database search and a simple Google search. BMC Medical Research Methodol. 20, 1–10. https://doi.org/10.1186/s12874-020-01084-x.

Dabthong, H., Warasart, M., Duma, P., Rakdej, P., Majaroen, N., Lilakiatsakun, W., 2021. Low COst Automated Os Security Audit Platform Using Robot Framework. Proc. 2021 Res. Invent. Innov. Congr. Innov. Electr. Electron. RI2C 2021 31–34. https://doi.org/10.1109/RI2C51727.2021.9559826.

David Audretsch, B., Belitski, M.The limits to open innovation and its impact on innovation performance 2022. https://doi.org/10.1016/j.technovation.2022.102519.

Deloitte. Auditing the RPA environment Our approach towards addressing risks in a BOT environment Risk Advisory 2018..

Deloitte. Creating an environment for apt and adept automation Seven-step progression of RPA risks and controls 2020. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/financial-reporting-rpa-risks.pdf (accessed April 28, 2024).

Devarajan, Y., 2018. A study of robotic process automation use cases today for Tomorrow's Business. Int. J. Comput. Tech. 5.

Durst S., Henschel T., editors. Knowledge risk management. 2020. (https://doi.org/10.1007/978-3-030-35121-2).

Eisenhardt, K.M., 1989. Building theories from case study research. Source. Acad. Manag. Rev. 14, 532–550.

ELEKS. Understanding and Eliminating Robotic Process Automation Security Risks 2022. https://eleks.com/blog/robotic-process-automation-security-risks/ (accessed May 1, 2022).

Financial Reporting Council. Auditor's Responsibilities for the Audit 2023. https://www.frc.org.uk/library/standards-codes-policy/audit-assurance-and-ethics/auditors-responsibilities-for-the-audit/ (accessed April 28, 2024).

Garousi, V., Felderer, M., Mäntylä, M.V., 2016. The need for multivocal literature reviews in software engineering: Complementing systematic literature reviews with grey literature, 01-03-June-2016 ACM Int. Conf. Proc. Ser.. https://doi.org/10.1145/2915970.2916008.

Garousi, V., Felderer, M., Mäntylä, M.V.Guidelines_for_including_grey_literature_and_conducting_multivocal_literature_reviews_in_software_engineering. Information_and_Software_Technology 2019;106:101–121. https://doi.org/10.1016/j.infsof.2018.09.006..

Gegenhuber, T., Mair, J., 2024. Open social innovation: taking stock and moving forward. Ind. Innov. 31, 130–157. https://doi.org/10.1080/13662716.2023.2271863.

Gotthardt, M., Koivulaakso, D., Paksoy, O., Saramo, C., Martikainen, M., Lehner, O., 2020. Current state and challenges in the implementation of smart robotic process automation in accounting and auditing. ACRN J. Financ. Risk Perspect. 9, 90–102. https://doi.org/10.35944/JOFRP.2020.9.1.007.

Griffiths, L., Pretorius, H.W., 2021. Implementing Robotic Process Automation for Auditing and Fraud Control. In: Communications in Computer and Information Science, 1477. CCIS, pp. 26–36. https://doi.org/10.1007/978-3-030-86761-4_3/FIGURES/1.

Hale, A., VanVleet, E., Butt, J., Hollis, T.The 'Power of With': Combining humans and machines to transform tax 2020. https://www.internationaltaxreview.com/article/

b1kblrgr0f73s7/the-power-of-with-combining-humans-and-machines-to-transform-tax (accessed February 4, 2022).
Handoko, B.L., Lindawati, A.S.L., Mustapha, M.Robotic process automation in audit 4.0. ACM International Conference Proceeding Series 2021a:128–132. https://doi.org/10.1145/3481127.3481140.
Handoko, B.L., Lindawati, A.S.L., Mustapha, M., 2021b. Robotic process automation in audit 4.0. Assoc. Comput. Mach. (ACM) 128–132. https://doi.org/10.1145/3481127.3481140.
Harsanto, B., Mulyana, A., Faisal, Y.A., Shandy, V.M., 2022. Open innovation for sustainability in the social enterprises: an empirical evidence, 2022;8:160 J. Open Innov.: Technol., Mark., Complex. Vol 8, 160. https://doi.org/10.3390/JOITMC8030160.
Hayes R., Wallage P., Eimers P. Principles of International Auditing and Assurance 4th Edition 2014. https://doi.org/10.5117/9789463720069.
Herrera, R., Burke, L., Diquez, E., Graff, D.RPA and the Path to Digitalization: What ' s in it for Internal Audit ? 2020..
Hevner, March, Park, Ram, 2004. Design science in information systems research. MIS Q. 28, 75. https://doi.org/10.2307/25148625.
Hollweck, T., Robert K, Yin, 2014. Case study research design and methods (5th ed.). Can. J. Program Eval. 2015 30, 108–110. https://doi.org/10.3138/cjpe.30.1.108.
Huang, F., Vasarhelyi, M.A., 2019. Applying robotic process automation (RPA) in auditing: A framework. Int. J. Account. Inf. Syst. 35, 100433 https://doi.org/10.1016/j.accinf.2019.100433.
Hugo Ciopages. Robotic Process Automation: The opportunity, risks and rewards 2016. https://www.ciopages.com/robotic-process-automation/ (accessed June 4, 2023).
Issa, H., Sun, T., Vasarhelyi, M.A., 2016. Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation. J. Emerg. Technol. Account. 13, 1–20. https://doi.org/10.2308/JETA-10511.
Javatpoint, 2021. Hist. RPA. (https://www.javatpoint.com/history-of-rpa) (accessed January 7, 2023).
Joshi, N.Leverage RPA, But Plan For Its Inherent Risks, Too! 2019. https://www.forbes.com/sites/cognitiveworld/2019/06/28/leverage-rpa-but-plan-for-its-inherent-risks-too/?sh=58aebc2a11d1 (accessed January 9, 2023).
Julka, S.What is Robotic Process Automation (RPA) ? Ultimate guide to RPA and how it's Driving Digital Transformation? 2021. https://www.nseit.com/resources/blogs/robotic-process-automation-ultimate-guide (accessed June 7, 2021).
Kamei, F.K., Soares, S., Pinto, G., 2018. The Use of Grey Literature Review as Evidence for Software Engineering.
Kitchenham, B., Charters, S., 2007. Guidelines_for_performing_systematic_literature_reviews_in_software_engineering. Technical_report,Ver23_EBSE_Technical_ReportEBSE.
KPMG. Balancing risk and change in Robotics Process Automation (RPA) transformation. 2018b..
KPMGKPMG. Managing risks of the growing RPA jungle 2018a:14.
Lievano-Martínez, F.A., Fernández-Ledesma, J.D., Burgos, D., Branch-Bedoya, J.W., Jimenez-Builes, J.A., 2022. Intelligent process automation: an application in manufacturing industry, 2022;14:8804 Sustainability Vol 14, 8804. https://doi.org/10.3390/SU14148804.
Lu, Q., Chesbrough, H.Measuring open innovation practices through topic modelling: Revisiting their impact on firm financial performance 2021. https://doi.org/10.1016/j.technovation.2021.102434.
Majchrzak, A., Bogers, M.L.A.M., Chesbrough, H., Holgersson, M.Creating and Capturing Value from Open Innovation: Humans, Firms, Platforms, and Ecosystems. Https://DoiOrg/101177/00081256231158830 2023;65:5–21. https://doi.org/10.1177/00081256231158830.
Mamede, H.S., Gonçalves Martins, C.M., Mira Da Silva, M., 2023. A lean approach to robotic process automation in banking. Heliyon 9, 18041. https://doi.org/10.1016/j.heliyon.2023.e18041.
Mandal, S., Amrein, C., Switchenko, J., Ryan Martin, R., Rosensweig, S.Robotic process automation: A primer for internal audit professionals. 2017.
March, S.T., Smith, G.F., 1995. Design and natural science research on information technology. Decis. Support Syst. 15, 251–266. https://doi.org/10.1016/0167-9236(94)00041-2.
Maria Gonçalves Martins C., Leitão Bignolas Mira da Silva Henrique Mamede M., Carlos Alves Pereira Monteiro Supervisor J., Leitão Bignolas Mira da Silva M. Robotic Process Automation A Lean Approach to RPA Information Systems and Computer Engineering Examination Committee. 2018.
Mennen, M.G., Van Tuyll, M.C., 2015. Dealing with future risks in the Netherlands: The National Security Strategy and the National Risk Assessment. J. Risk Res 18, 860–876. https://doi.org/10.1080/13669877.2014.923028.
MetricstreamMetricstream. Audit Performance Measurement - Insights 2023. https://www.metricstream.com/insights/audit_performance_measurement.htm (accessed March 2, 2023).
Minnaar, D., Smith, M.Internal Audit and Robotic Process Automation 2018:1–16.
Mittal M.R.P.A. (Robotics Process Automation) - An enabler of Business Continuity 2020. (https://www.linkedin.com/pulse/rpa-enabler-business-continuity-manish-mittal/) (accessed July 25, 2021).
Moffitt, K.C., Rozario, A.M., Vasarhelyi, M.A., 2018a. Robotic process automation for auditing. J. Emerg. Technol. Account. 15, 1–10. https://doi.org/10.2308/JETA-10589.
Moffitt, K.C., Rozario, A.M., Vasarhelyi, M.A., 2018b. Robotic process automation for auditing. J. Emerg. Technol. Account. 15, 1–10. https://doi.org/10.2308/jeta-10589.
Murphy, M.L., 2020. Assessing audit risks during the pandemic. J. Account. (https://www.journalofaccountancy.com/news/2020/dec/assess-audit-risks-during-coronavirus-pandemic.html) (accessed October 22, 2023).
Myers, M.D., 2013. Second edition. Qualitative Research in Business and Management Second Edition. SAGE Publications Ltd.
Myers, M.D., Newman, M., 2007. The qualitative interview in IS research: examining the craft. Inf. Organ. 17, 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001.
Namchoochai, R., Kiattisin, S., Darakorn Na Ayuthaya, S., Arunthari, S., 2020. Elimination of FinTech Risks to Achieve Sustainable Quality Improvement. Wirel. Pers. Commun. 115, 3199–3214. https://doi.org/10.1007/s11277-020-07201-9.
Nunes T., Leite J., Pedrosa I. Intelligent Process Automation: An Overview over the Future of Auditing. Iberian Conference on Information Systems and Technologies, CISTI 2020;2020-June. (https://doi.org/10.23919/CISTI49556.2020.9140969).
Ogawa, R.T., Malen, B., 1991. Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method. Rev. Educ. Res 61, 265–286. https://doi.org/10.3102/00346543061003265.
Olson, D.L., Wu, D.D., 2021. Enterp. risk Manag. https://doi.org/10.1142/6732.
Peffers, K., Tuunanen, T., Gengler, C.E., Rossi, M., Hui, W., Virtanen, V., , 2006. The design science research process: a model for producing and presenting information systems research.
Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A design science research methodology for information systems research. J. Manag. Inf. Syst. 24, 45–77. https://doi.org/10.2753/MIS0742-1222240302.
Peñarroya-Farell, M., Miralles, F., 2021. Business model dynamics from interaction with open innovation. J. Open Innov.: Technol., Mark., Complex. 7, 81 https://doi.org/10.3390/JOITMC7010081.
Peñarroya-Farell, M., Miralles, F., Joseph Yun, J., Salle, L.Business Model Dynamics from Interaction with Open Innovation 2021. https://doi.org/10.3390/joitmc7010081.
Pluzhnikov, O., 2020. Top 10 security risks of RPA. Eleks.
Pokhrel, A., Katta, V., Colomo-Palacios, R., 2020. Digital twin for cybersecurity incident prediction: a multivocal literature review. Proc. - 2020 IEEE/ACM 42nd Int. Conf. Softw. Eng. Workshops, ICSEW 2020 671–678. https://doi.org/10.1145/3387940.3392199.
Raval, V., Smith, E., 2020. Organizational RPA Adoption and Internal Auditing. ISACA J. 2, 13–16.
Rezaee, Z., Sharbatoghlie, A., Elam, R., Mcmickle, P.L.Continuous Auditing: Building Automated Auditing Capability. vol. 21. 2002.
Rosemann, M., Vessey, I., 2008. Toward improving the relevance of information systems research to practice: The role of applicability checks. MIS Q 32, 7–22. https://doi.org/10.2307/25148826.
Sikora, S., Hurley, B., Tharakan, A.G.Automation with intelligence Pursuing organisation-wide reimagination. 2019.
Skantze, J.A. Continuous Auditing – Internal Audit at a Crossroads?, 2019.
Software Testing Help. 10 Most Popular Robotic Process Automation RPA Tools in 2023 2023. https://www.softwaretestinghelp.com/Robotic-Process-Automation-Tools/ (accessed October 22, 2023)..
Stansfield, C., Dickson, K., Bangpan, M., 2016. Exploring_issues_in_the_conduct_of_website_searching_and_other_online_sources_for_systematic_reviews:How_can_we_be_systematic? Systematic_Reviews 5, 1–9. https://doi.org/10.1186/s13643-016-0371-9.
Steinhoff, J.C., Lewis, A.C., Everson, K.E., 2018. The march of the robots. J. Gov. Financ. Manag. https://doi.org/10.1787/244551P6-EN.
Steinhoff, J., Lewis, A., Everson, K., 2019. The march of the robots. J. Gov. Financ Manag. 26–33.
Stephen S. Audit Report Issue Email Template. (Https://WwwStudocuCom/En-Us/Document/the-University-of-Texas-at-Dallas/Auditing/Audit-Report-Issue-Email-Template/6320637) 2020.
Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S.J.J., Ouyang, C., et al., 2020a. Robotic Process Automation: Contemporary themes and challenges. Comput. Ind. 115, 103162 https://doi.org/10.1016/J.COMPIND.2019.103162.
Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S.J.J., Ouyang, C., et al., 2020b. Robotic Process Automation: Contemporary themes and challenges. Comput. Ind. 115 https://doi.org/10.1016/j.compind.2019.103162.
Szalony, S., Salkin, P., Sewell, K., 2019. The 3 Rs of Finance Automation: RPA, Risk, Rewards - WSJ. https://deloitte.wsj.com/articles/the-3-rs-of-finance-automation-rpa-risk-rewards-01574283372 (accessed May 27, 2023).
The Institute of Internal Auditors. GTAG: Continuous Auditing 2019. https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-continuous-auditing/ (accessed November 25, 2023).
The Internal Auditor. Internal Audit documents and templates 2023. https://www.theinternalauditor.org/Documents/ (accessed August 9, 2023).
The New Frontier Of Automation: Enterprise RPA. 2017.
Van den Oever, B.Method for estimating the impact of Robotic Process Automation implementations on business processes. 2020.
Vasarhelyi, M.A., Alles, M.G., Kogan, A., 2004. Principles of analytic monitoring for continuous assurance. J. Emerg. Technol. Account. 1, 1–21. https://doi.org/10.2308/JETA.2004.1.1.1.
Vasarhelyi, M.A., Alles, M., Kuenkaiknew, S., Littley, J., 2012. The acceptance and adoption of continuous auditing by internal auditors: a micro analysis. Int. J. Account. Inf. Syst. 13, 267–281. https://doi.org/10.1016/j.accinf.2012.06.011.
Violino, B. 6 hidden risks of IT automation 2020. https://www.cio.com/article/190962/6-hidden-risks-of-it-automation.html (accessed January 9, 2023).
Vlăduț, G., Tănase, N.M., Caramihai, M., Purcărea, A.A., 2018. Innovation Audit for business excellence. Proc. Int. Conf. Bus. Excell. 12, 1026–1037. https://doi.org/10.2478/picbe-2018-0092.
V-Soft ConsultingV-Soft Consulting. Session 08 - Business Continuity Powered by AI and Automation 2020. https://www.youtube.com/watch?v=rWVchFNcw34 (accessed September 13, 2021).

Widuri, R., Handoko, B.L., Prabowo, I.C., 2019. Adoption of Information Technology in Public Accounting Firm. Proceedings of the 2019 4th International Conference on Big Data and Computing ICBDC 2019. ACM Press, New York, New York, USA, pp. 198–202. https://doi.org/10.1145/3335484.3335500.

Wojciechowska-Filipek, S., 2019b. Automation of the process of handling enquiries concerning information constituting a bank secret. Banks Bank Syst. 14, 175–186. https://doi.org/10.21511/bbs.14(3).2019.15.

Wojciechowska-Filipek, S., 2019a. Automation of the process of handling enquiries concerning information constituting a bank secret. Banks Bank Syst. 14, 175–186. https://doi.org/10.21511/BBS.14(3).2019.15.

Yun, J.H.J., Ahn, H.J., Lee, D.S., Park, K.B., Zhao, X., 2022. Inter-rationality; Modeling of bounded rationality in open innovation dynamics. Technol. Forecast Soc. Change 184. https://doi.org/10.1016/j.techfore.2022.122015.

Zinca, C.-I., 2016. Measuring the value of internal audit in the banking industry. Audit Financ. XIV, 1009–1024. https://doi.org/10.20869/AUDITF/2016/141/1009.

Chapter 5

Article nr. #4 – “Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective.”

This article provides an important perspective on the risks associated with the adoption of RPA from a business continuity perspective. It underscores the significant shift towards digital transformation and highlights how RPA has become increasingly integral to organizational operations. Despite its potential benefits in terms of cost reduction and efficiency, RPA also introduces notable risks due to its dependence on software components governed by predefined rules. The research identifies and analyzes key risk factors that may emerge from the integration of RPA in organizational contexts. It classifies these risks into various categories, such as operational, strategic, regulatory, and security risks, and examines how they intersect with the fundamental concepts underpinning RPA. The study provides an in-depth exploration of how automation technology's inherent risks can potentially disrupt critical business processes if not carefully managed.

Furthermore, the article lays out a framework for understanding and mitigating these risks to safeguard business continuity. It provides researchers and practitioners with structured insights into how to address the challenges of automation, emphasizing the importance of aligning automation strategies with robust risk management practices. The research emphasizes the necessity for organizations to carefully assess and adapt their risk management frameworks to ensure that the adoption of RPA enhances, rather than undermines, business continuity.

Article Details:

- Title: "Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective."
- Journal: Schmalenbach Journal of Business Research.
- Submission Date: 04/29/2023
- Publisher: Springer.
- Scimago Journal Rank: Quartile 1 – Business, Management and Accounting

Schmalenbach Journal of Business Research

Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective

--Manuscript Draft--

Manuscript Number:	SBUR-D-24-00217	
Full Title:	Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective	
Article Type:	Original Article	
Funding Information:	COPELABS	PhD Student José Cascais Brás
Abstract:	The global shift towards digital transformation, exemplified by organisations' increasing adoption of Robotic Process Automation for process automation, has been noteworthy. This transformation yields evident advantages in terms of cost reduction and heightened operational efficiency, achieved through the delegation of repetitive, error-prone tasks from human workers to automated systems. However, this paradigm shift is not without its attendant risks, as it hinges on the automation of processes executed by software components that operate solely on pre-defined rules, lacking inherent decision-making capabilities. Thus, the present research centers on examining the risk factors that may accompany the integration of Robotic Process Automation in organisational contexts, aiming to comprehensively identify and analyse their principal determinants. This investigation contributes with a list of risk factors, organized, mapped, and grouped into categories, and how they are interconnected with the fundamental concepts supporting RPA. In this sense, this study will help future researchers to identify the risks associated with Robotic Process Automation to define actions that avoid negative impacts and allow Business Continuity.	
Corresponding Author:	José Cascais Brás ISCTE-Instituto Universitário de Lisboa: ISCTE-Instituto Universitario de Lisboa PORTUGAL	
Corresponding Author E-Mail:	jose_manuel_bras@iscte-iul.pt	
Corresponding Author Secondary Information:		
Corresponding Author's Institution:	ISCTE-Instituto Universitário de Lisboa: ISCTE-Instituto Universitario de Lisboa	
Corresponding Author's Secondary Institution:		
First Author:	José Cascais Brás	
First Author Secondary Information:		
Order of Authors:	José Cascais Brás	
	Ruben Filipe Pereira	
	Isaias Scalabrin Bianchi	
	António Pedro Brites	
	Rui Ribeiro	
Order of Authors Secondary Information:		
Opposed Reviewers:		
Additional Information:		
Question	Response	
Does this manuscript belong to a special issue?	No	

Risk Impacts Related to Robotic Process Automation: A Business Continuity Perspective

Abstract

The global shift towards digital transformation, exemplified by organisations' increasing adoption of Robotic Process Automation for process automation, has been noteworthy. This transformation yields evident advantages in terms of cost reduction and heightened operational efficiency, achieved through the delegation of repetitive, error-prone tasks from human workers to automated systems. However, this paradigm shift is not without its attendant risks, as it hinges on the automation of processes executed by software components that operate solely on pre-defined rules, lacking inherent decision-making capabilities. Thus, the present research centers on examining the risk factors that may accompany the integration of Robotic Process Automation in organisational contexts, aiming to comprehensively identify and analyse their principal determinants. This investigation contributes with a list of risk factors, organized, mapped, and grouped into categories, and how they are interconnected with the fundamental concepts supporting RPA. In this sense, this study will help future researchers to identify the risks associated with Robotic Process Automation to define actions that avoid negative impacts and allow Business Continuity.

Keywords: business continuity; governance; risk; compliance; auditing; robotic process automation; intelligent process automation; business process management

1 Introduction

The reality of our time shows that organisations, to remain competitive, have to keep up to date in digital terms, being forced to carry out profound transformations in them. However, this digital transformation (DT) offers organisations opportunities to stand out using disruptive digital technologies [1]. The adoption of disruptive technologies increasingly plays an important role in all areas of business and is seen as a key factor in changing the way companies create value and gain competitive advantage [2]. To reduce the time to launch new products and services on the market, companies were forced to reinvent their business models, forcing rapid technological changes.

Robotic Process Automation (RPA) is a technological innovation that addresses the needs of organisations to keep up with the high pace of technological change [3]. Automating repetitive tasks, allows employees to make better use of their time on more complex tasks, thus bringing more value to the organisation [4]. With the use of RPA, there is a strong impact on a business's operations and competitive positioning on several fronts: economic value, workforce advantages, quality improvements, flexible execution, speed, and agility [5]. Recently, COVID-19 highlighted the importance of RPA by allowing to replace workers in organisations who were unable to work, due to illness or being in isolation, allowing these companies to continue their business [6–9].

Although there is much information available on the benefits of using RPA due to the high demand in the business world, there are also risks, however, these risks have been few mentioned by authors in the scientific community [3, 10].

RPA is a secure solution to mitigate human errors while executing business processes, but RPA is also subject to human errors and can easily pose risks to the organisation because it is a tool of consistent and continuous action, where any error can become a systematic and widespread problem in the underlying business process and associated dataset, thus jeopardizing business continuity[11, 12]. Therefore, this study aims to identify the risks associated with RPA, create a framework to develop a risk assessment strategy and support business continuity.

An important study done recently regarding RPA implementation presented a conceptual model with an end-to-end perspective regarding RPA Case Studies (CS) [3]. It synthetizes the main topics related to RPA, such as the benefits, disadvantages, suitable process criteria, future challenges, and opportunities, where a conceptual model on the relationships between RPA main topics was performed, providing a schema for conducting CSs. In this conceptual model, shown in Figure 1, three steps were identified (strategic goals, process assessment, and tactical evaluation) and the factors that influence them (benefits, disadvantages, selection criteria, future challenges, and future opportunities).

Fig. 1 – RPA Conceptual model of main concepts around RPA and their relationships (adapted from [13])

According to the authors, these factors must be considered, so that the implementation of process automation with RPA can be effective.

The objective of this study is to discern, from a Business Continuity standpoint, the key risk factors and their potential implications on the core principles associated with the main concepts around RPA, answering the following research questions: (1) "What constitutes the principal risk factors in the context of RPA implementations?", (2) "In what manner are these risk factors interconnected with the fundamental concepts of RPA implementation?". The research will prioritize synthesizing diverse perspectives on RPA risks from a wide range of sources, including academic articles, industry reports, and case studies. This approach aims to capture the multifaceted nature of RPA risks, understanding the variations in risk perceptions across different stakeholders. It will also explore the evolution of these risks over time and through diverse technological advancements, providing a holistic view of the RPA risk landscape, aiming to build on the foundational work of the article by expanding the understanding of RPA risks, developing comprehensive risk management strategies, and contributing to the safe, efficient, and effective adoption of RPA technologies in organizations.

The remainder of this paper is comprised as follows. Section 2 presents the theoretical background. Section 3 describes the Multivocal Literature Review (MLR). Section 4 presents the review report. Section 5 presents the evaluation and discussion of the results. Finally, section 6 presents the conclusion and limitations of this study and future research.

2 Theoretical Background

This section is dedicated to the Background and seeks to theoretically frame the object of the study. Through key concepts, it is possible to clarify critical domains about RPA, potential risks, Business Continuity, and how RPA risk factors impact business continuity.

2.1. Business Continuity Management

One of the processes associated with management is Business Continuity, whose objective is to identify potential threats that may cause an interruption to an organisation's business. This process has become increasingly complex over time due to the increase in the complexity of information systems, the incorporation of new business processes, and the constant emergence of new threats to organisations.

Compared to other business management disciplines, Business Continuity Management (BCM) is relatively recent, appearing in the sixties as a way of safeguarding the company's investments in technology and evolving, based on emerging legislation and standards until 2001[14–25]. In 2012, became an International Organisation for Standardization (ISO)[26], and its most recent update, ISO 22332 [27] provides us with guidelines for developing business continuity plans and procedures. Figure 2 illustrates the evolution and the major milestones in this process.

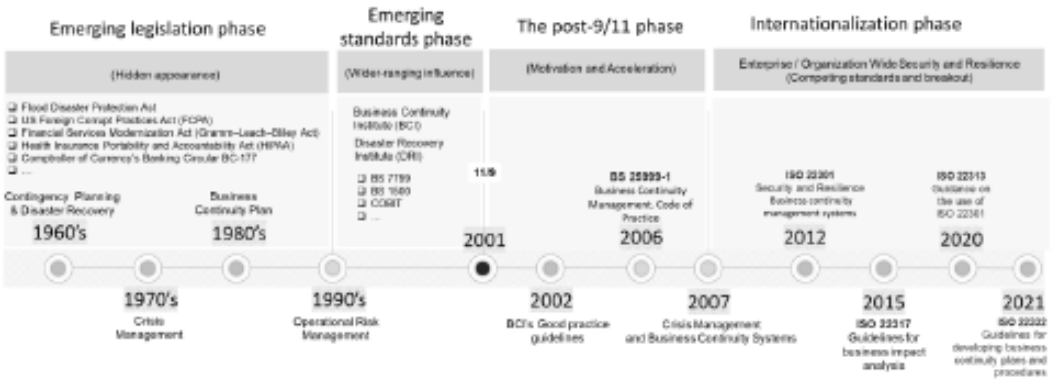


Fig. 2 - BCM evolution phases (adapted from[28])

Business continuity has become more relevant over time due to risks that have become real events: 9/11 in the USA, climate changes that affect the planet, and the recent COVID-19 pandemic, which have all shaped the path of BCM (Figure 2) [29]. Issues related to Security, Resilience, and Business Continuity, are important topics for organisations today due to the growing increase in risks linked to the current situation.

Business Continuity mainly establishes the strategies, procedures, and critical actions required to successfully respond to a crisis. In addition, it evaluates how well an organisation responds to unexpected disasters, disruptions, or sudden changes to its business environment. As crises may result from natural disasters, catastrophes, or just a simple accident that can interrupt services, resulting in the partial or total loss of business, a Business Continuity Plan (BCP) must address all possible situations to mitigate or assume their risk. Therefore, it is quite relevant to address all risks involving RPA implementations [30]. Risk assessment is part of Business Continuity practice, where the risks are identified, managed, and reduced [31].

Legislation like NIS2[32, 33] and DORA [33] highlight the importance of BCM and Risk Management as they demand the identification and protection of critical Information Technology (IT) systems, implementation of incident response and business continuity plans, conduction of regular testing and risk assessments, establishing a reporting framework for major incidents, Risk management of third-party Information and communication technology (ICT) providers, incident reporting, testing and exercises, IT and cyber risk governance.

2.2. Robotic Process Automation and Intelligent Process Automation

These two terms are very similar, but while RPA is focused on automating repetitive tasks and processes based solely on rules, intelligent automation by its very nature incorporates a vast array of Emerging Technologies (ET), such as Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), Structured Data Interaction, and Intelligent Document Processing.

RPA is a relatively recent technology used to automate a combination of processes, tasks, activities, or services, with graphical user interfaces that are choreographed to interact with almost any type

of system as a human user would [34, 35]. Both scientific research and the media highlight the potential of RPA for increasing the efficiency of processes. Since the development of RPA solutions requires low levels of programming experience, with low implementation costs and a very fast return on investments, these solutions are suitable for a very wide range of processes and result in very high-efficiency gains. Hence, the technology has attracted interest in the business world, with several examples of successful implementation [36].

The first approach to this technology (Process Automation) involved replacing the routine or strictly transactional processes performed by humans. As this technology evolved, capabilities related to ML and cognitive computing were added, with increasingly sophisticated rule mechanisms, and it started to be able to perform more complex human tasks, including evaluation, reasoning, decision-making, and compliance with probabilistic and/or deterministic process requirements in dynamic contexts. Intelligent Process Automation is thus the evolution of simpler repetitive tasks, in which new capabilities are added with more sophisticated and complex procedures.

Companies continually seek to lower costs and increase in efficiency to succeed in an uncertain, turbulent, and competitive environment. Information technology has been, for decades, one of the main strategies adopted to achieve these goals. But process automation can always go further, better articulating different subsystems, or accelerating the connection from analogic to digital [37].

The introduction of processes that seek to improve the quality of the product/service offered and cost retention are some of the essential paradigms in the eyes of an organisation, which can be achieved by creating a connection point between partners/employees and customers.

However, since these automated processes may highlight some risks, this study aims to conduct a survey of the risks in order to identify them, contributing in the scientific community so that companies and future experts can drive actions that mitigate potential threats in business continuity [25].

3 Methodology

The MLR [38] is similar to the Systematic Literature Review (SLR) [39, 40] and aims to incorporate the so-called "grey literature" in order to supplement the published (formal) literature. MLRs are SLRs that include both scholarly writing (also known as academic writing or formal writing) and the (informal) grey literature (GL). Scholarly writing is the genre of writing used in all academic fields. GL is considered a multisource of information, which may exist in the form of blogs, videos, webpages, and white papers that are produced outside academic forums and are not subject to any quality control mechanism (e.g. the peer review process) before publication.

By including information that normally would not be taken into account due to its "grey" nature [38], MLRs are important for the completeness of the research. An MLR in a given subject field is essentially a combination of the sources that would be studied in an SLR and a GLR in the same field. Thus, an MLR is, in principle, expected to provide a more complete picture of the evidence in a given field. Figure 3 represents the relationship between SLR, GLR and MLR.

Fig. 3 - The relationship between SLR, GLR and MLR

Due to the fast evolution of IT, several researchers have already realized that including the GLR brings benefits to the study review, because it is a way to add value and knowledge without compromising the viability of the information. Some examples of successful studies (linked to the IT area) which also used MLR already exist [41][42][43]. This way we could confirm the practical usefulness of this method

and apply it in this research, contributing to the diversity of different sources of knowledge currently available in various forms, with different perspectives and objectives [44].

The research of this MLR aims to discover which are the major risk factors of RPA implementation described by the various professionals in the field and to be able to detail them thoroughly by finding out if there is a consensus on the best way to avoid these risks during its implementation. For this, we have the need to expand this study beyond the limits of scientific knowledge. Thus, MLR gives us this opportunity and manages at the same time to maintain a rigorous quality in the process of analysis of this literature [44].

In Table 1, we can observe the separation of the different sources of the "White" and "Grey" literature, and the set of the two forms of the MLR. It should be noted that for greater credibility of the data, literature that corresponds to ideas, concepts, and thoughts, social networks, tweets, and emails were excluded [45].

Table 1 - Spectrum of the "White", "Grey" and Excluded literature (adapted from [38])

"White" literature	"Grey" literature	"Black" or other types of literature (excluded)
Papers published in journals Conference proceedings Books	Preprints e-Prints Lectures Datasets Government documents Standards White papers Technical reports Blogs Audio-video media	Ideas Concepts Thoughts

The MLR workflow is summarized in Figure 5 and has three phases. The initial phase of the research ("Planning the MLR") comprises two steps:

- Determining the need for an MLR for the given topic
- Defining the MLR goal and setting up the research questions

There are numerous guidelines for conducting an SLR study. However, several phases of MLR do not coincide with traditional SLRs. One of these is the process of assessing the quality of the source of information and its investigation. Therefore, we will partially use the SLR guidelines to carry out this MLR. We can observe in Figure 4, the structure of the guidelines for this MLR, which shows the planning, conducting, and reporting exactly as was proposed by Garousi et al [45].

With the implementation of this model, it is expected that the grey literature will provide us with important knowledge about the risks of implementing the RPA, not disregarding that this will bring new challenges when including such literature, as the knowledge provided is often based on the experience and opinion of those working in the field. For this reason, in this research, we will use systematic guidelines to perform MLR [46] and thus achieve a consistent and concise data collection similar to what is done in an SLR, applying to the inclusion and exclusion criteria in the results obtained through the world's most well-known search engine called Google.

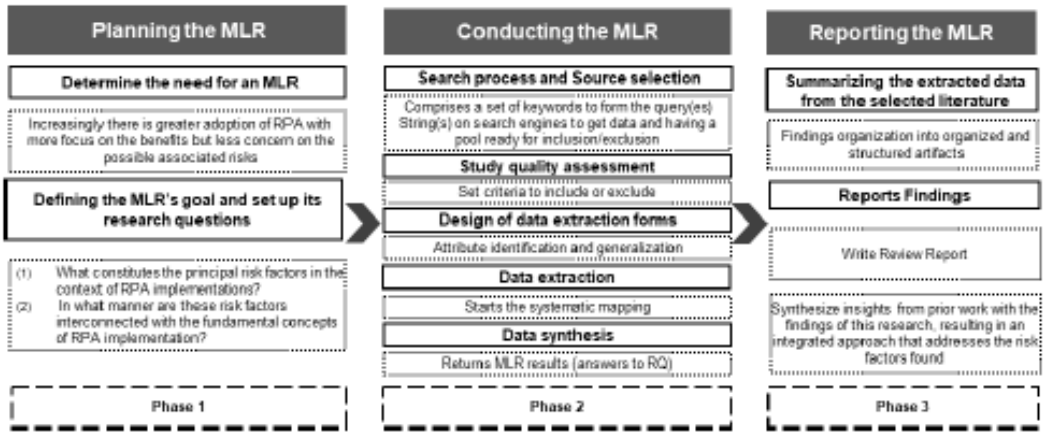


Fig. 4 - MLR phases and steps adopted in this research (adapted from [38])

3.1. Planning the Review

This section represents the first phase of the MLR implementation. It starts with the motivation that led this subject to be studied, then what are its objectives, and what are the research questions we propose to answer with this research.

3.1.1. Motivation

The Covid-19 pandemic greatly impacted organisations, forcing them to adapt to a new reality very quickly. This quick adaptation is reflected in the "Digital Transformation" of processes that, in a way, increases the potential for emerging technological risks associated with the introduction of new technology into business processes. Organisations needed to accelerate the use of digital technology and replace various business processes previously performed in what may be called a "traditional" way with alternative, complementary ways of using technology [47]. The most prominent examples were related to work roles that were downsized or replaced with technology to mitigate infection risks while maintaining productivity. For example, during the pandemic, online channels have become the salvation for consumers looking for products and companies looking for alternative ways to place their products and services on the market. This highlights the need to implement digital transformation solutions to answer the challenges organisations face today. Figure 5 expresses the interest that RPA started to have in 2004, illustrating that 2016 is when it started to show some impact on user searches and reached its highest point during the pandemic.

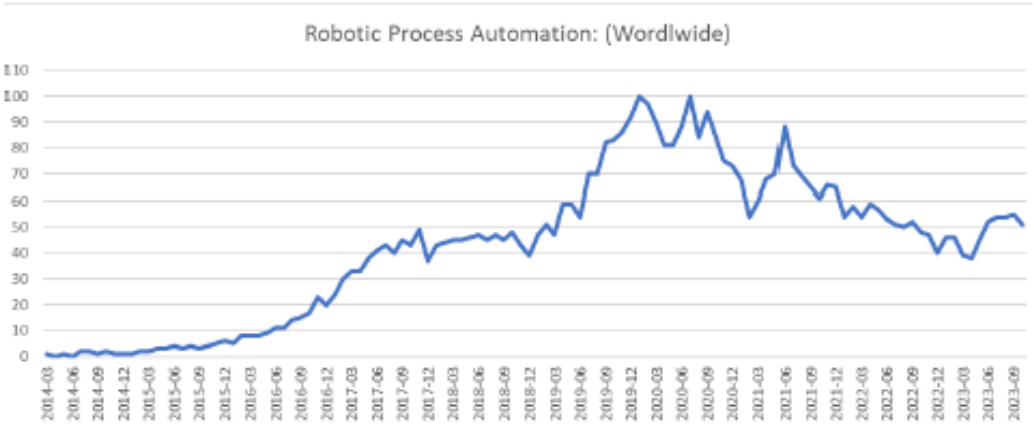


Fig. 5- interest of Robotic Process Automation over time – google trends [48]

3.1.2. Establishing the need for an MLR

RPA has been attracting a lot of attention from the corporate world. However, although it is a popular topic in the corporate world, academic research lacks a deeper theoretical analysis of RPA [49]. As a niche area of IT, literature on RPA is rather sparse in terms of its impact on organisations and, consequently on business continuity. Further investigation should involve a comprehensive assessment of this technology, identifying risks and revealing additional factors that influence the adoption of RPA technology [50].

Since RPA/IPA is being explored more within industry than academia, resulting in important inputs [51–54], an MLR expands the origins of the sources to identify and map the most important risk areas related to this topic.

3.1.3. Review Protocol

The review protocol specifies the research question being addressed and the methods that will be used to perform the review. To find the maximum number of studies related to the research question, a search strategy was used to detect as much of the relevant literature as possible using multiple keywords and datasets.

Keywords:

- Robotic Process Automation / Intelligent Process Automation / Risks

Search String:

- (Robotic Process Automation OR Intelligent Process Automation) AND Risks)

Datasets:

- IEEE Xplore (https://ieeexplore.ieee.org)
- ACM DL (https://dl.acm.org)
- Scopus (https://scopus.com)
- Web of Science (https://apps.webofknowledge.com)
- EBSCO (https://search.ebscohost.com)
- Springer (https://springer.com)
- Google Scholar (https://scholar.google.com)
- Google Search (https://google.com)

The limitation of Google Search concerning the replicability of searches conducted at a specific time was considered. However, some scholars argue that website search methodologies may vary, underscoring the greater significance of adopting a well-considered rationale for the research process. This entails taking into consideration the specific goals and objectives of each review, rather than rigidly adhering to a singular method. Accordingly, meticulous planning and execution of the research, along with the systematic screening of results and the implementation of effective management structures, are imperative for this approach [55].

As a result, conducting a comprehensive grey literature search employing at least one conventional search engine (e.g., Google, Yahoo, or Bing) is recommended, extending the examination to the first 12 pages rather than confining it to the initial 5 pages. Additionally, a thorough exploration of academic databases closely aligned with the subject matter in question is advised. This dual-pronged approach ensures that all pertinent literature is duly considered, ultimately contributing to more comprehensive and robust conclusions [56, 57].

An inclusion and exclusion criteria were adopted to identify the relevant literature for this MLR. The screening criteria for including or excluding articles for this research are summarized and illustrated in Table 2.

Table 2 - Inclusion and exclusion criteria used.

Inclusion criteria	Exclusion criteria
Related to main keywords	Not related to RPA, IA or IPA and Business Continuity
Process automation or business continuity	Paper not in English
Title, abstract, key contents or subject relevance	Documents with publication date earlier than 2017
Journals, conference papers, blogs or grey literature	Vendor tool advertisements
Documents in English	Papers by unidentified authors
Limit results to first 12 pages of Google Search	No publication date

To maximize the incorporation of pertinent sources, the practice of both backward and forward snowballing was employed, following the guidance outlined in systematic review protocols [58], to the set of articles already in the pool. Within this context, snowballing entails the utilization of an article's reference list (termed backward snowballing) or citations within an article to identify supplementary articles (referred to as forward snowballing) [58].

A software package, specifically Mendeley, was employed to conduct literature searches and collation. This application guarantees the acquisition of distinct and non-repetitive results, as it can identify and remove duplicate entries. Consequently, this functionality addresses issues related to consistency in the retrieved and amassed results. Additionally, Mendeley assists in categorizing the results into distinct sets based on query strings and classifications into academic or grey literature. Moreover, it streamlines the process of retrieving results from the respective unique identification sets (comprising both academic and grey literature) for seamless integration into the Systematic Literature Review (MLR) process.

3.1.4. Defining the MLR goal

As seen in Figure 4, the MLR planning phase is subdivided into two phases, and after completion of the first phase, where the need for the MLR was established in relation to the topic, a main goal was defined, which aims to identify the principal risks associated with the use and implementation of the RPA.

3.2. Conducting the review

This section describes how the review was conducted, which is the second phase of the process. In this stage, the research is carried out by searching for information in selected databases using pre-defined queries and analysing the extracted data.

3.2.1. Selection of studies

This section presents how the filtering of the articles was done and the documents' final result, including figures and tables representing the extraction process. All filters applied are cumulative.

The first filtering consists of searching for exact matches, thus looking for the exact set of keywords, without the words being searched individually and separately. At this stage, a total of 671 articles were retained in all databases.

In the second filtering, a search cut-off date was applied, where only articles dated 2016 or later were retained, thus avoiding articles that are not directly related to the intended subject, as can be seen in Figure 6, 2016 was the date when the subject started to have some relevance on the Internet and, consequently, in the scientific community. At this stage, 632 articles remained.

After applying the search deadline, the search for keywords with exact matches only in the abstract was started, thus significantly reducing the dataset, and obtaining documents very close to the intended subject, which represents a total of 260 articles. It was impossible to apply this filter in three databases, Springer, Google Scholar, and Google Search.

To ensure the reliability of the documents, a manual review was performed in this filtering phase, where it was checked if it was possible to access the document without any restriction and also if the

document was complete and without missing parts, as happened in the links obtained in Google Search, which were sometimes parts of books or articles without access permissions. Thus, at this stage, 200 articles are filtered.

The next filtering process was done through the Mendeley software, where all the documents up to that point were loaded, and using a feature of the program, all duplicate documents were eliminated, leaving 189 unique articles.

Finally, the inclusion and exclusion criteria were applied, where the criteria were previously defined as shown in Table 2. This filter was applied mainly for the search in the Google Search database, because, in this way, it was guaranteed that only articles written in English, which mentioned the intended topic, were extracted, and articles that had no author, thoughts, or advertisements and posts defined were excluded. After applying this last filter, 107 articles directly related to this study remained.

As can be seen in Figure 6, the whole process is in an illustrative and easy-to-understand way, where all the databases used, the filters applied, and the result of this process are represented.

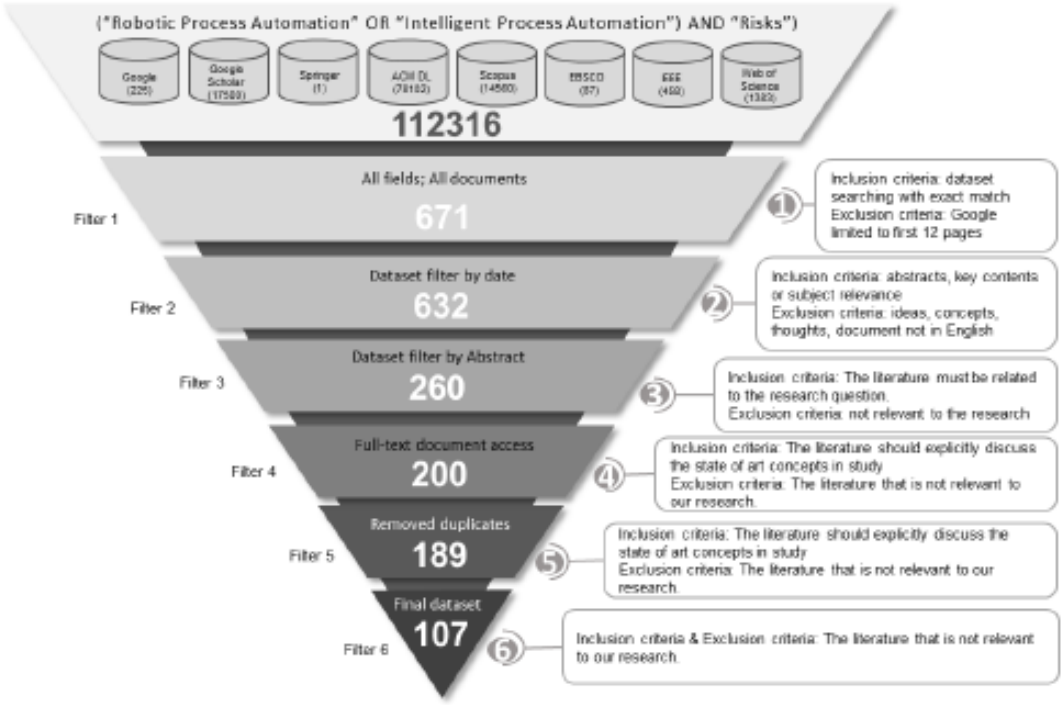


Fig. 6 - Followed Multivocal Literature Review process (adapted from [59])

3.2.2. Data Extraction Analysis

In this section, a meticulous analysis of the final selection of publications was conducted, explicitly delineating the documents extracted from each database after the application of all filtering criteria. This analysis affords a clear distinction between the number of articles constituting the "grey" literature, encompassing web pages and technical reports, and those classified under the category of "white" literature, denoting conventional scientific articles and books.

Table 3 provides a comprehensive overview of the number of articles retrieved from each database, presenting the outcomes after the application of individual filtering criteria. Notably, all filtering criteria played a pivotal role in constraining the information to exclusively encompass pertinent articles for this investigation. Notably, Table 3 elucidates that before implementing any filters, a total of 112,316 articles were identified solely through keyword searches.

Search String:

- (Robotic Process Automation OR Intelligent Process Automation) AND Risks

Table 3 - Filters used in the MLR protocol

Base de Dados	Initial	F1	F2	F3	F4	F5	F6
IEEE Xplore	458	4	4	3	3	3	1
ACM DL	78102	30	22	1	1	1	1
Scopus	14560	292	292	21	13	13	6
Web of Science	1383	75	47	3	3	3	1
EBSCO	87	77	77	42	14	8	2
Springer	1	1	1	1	1	1	1
Google Scholar	17500	11	11	11	11	11	11
Google Search	225	181	178	178	154	149	84
Total	**112316**	**671**	**632**	**260**	**200**	**189**	**107**

**Underlined means the number came transferred from the previous filtering due to the impossibility of executing F3*

Initial: Search keywords without filtering
F1: Query All fields with exact match
F2: Query All fields with exact match and date ≥ 2016
F3: Query Abstract with exact match and date ≥ 2016
F4: Full-text Document access
F5: Remove duplicates
F6: Inclusion and Exclusion criteria

4 Reporting the review

The objective of this research is to identify the principal risk factors associated with the use and implementation of RPA, and to facilitate the framing of all these risk factors, groups were created to give us a more peripheral vision of their impact. From here it was also possible to understand which ones have the greatest impact based on existing extractions from the grey and academic literature. Thus, the following risk factors groups aim to respond in detail to the goals defined in this research, research questions one and two.

4.1. Risk Factors Groups

To implement RPA, it is necessary to know how to face the risks it warns about and how to frame them correctly. And according to the research done for this study, several authors have framed the risks into different major groups [60–62]. Groups where, in general, there is a consensus that the main risks can be categorized. A first prototype of risk groups was formed, starting with Management, Governance, Operational, Technology, Security, Resources, Business Continuity and Data, which represents the eight groups mentioned.

Next, it was verified that there was a great concern with some groups of Risk factors - Management that represents 20,25%, Governance 15,19%, Operational 15,19%, Technology 13,92%, Security 11,39%, Resources 10,13%, Business Continuity 8,86% and Data 5,06% [40][41][42], presented in Figure 7.

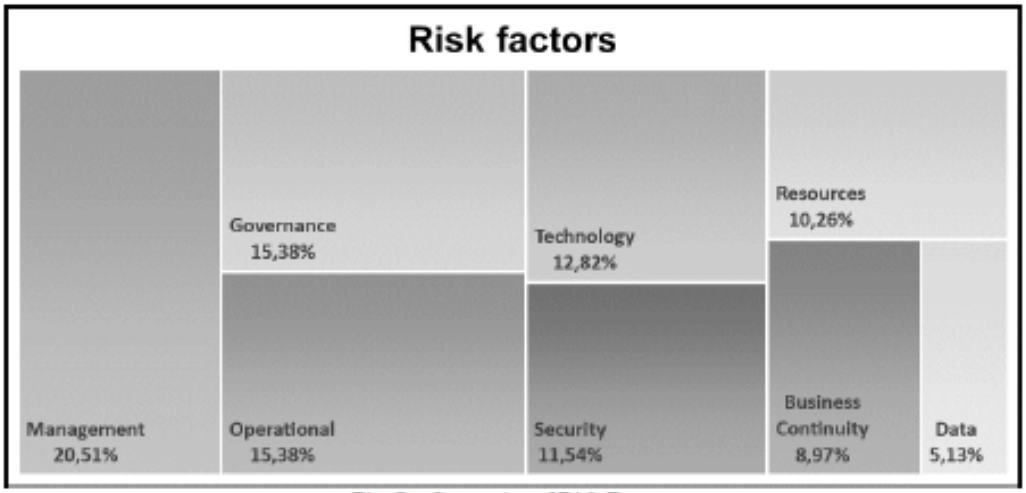


Fig. 7 – Categories of Risk Factors

Management Risk Factors

In the realm of Management regarding RPA, critical pitfalls can impede the realization of its transformative potential. One prominent stumbling block is the neglect of comprehensive documentation (Poor documentation), present in three references, a practice that can precipitate a cascade of setbacks [60, 63, 64]. Also, inadequate documentation manifests as suboptimal design, thereby catalysing complications during the execution and maintenance phases. This gap obstructs process reusability and introduces an insidious ripple effect, intensifying inefficiencies and entailing costly corrective measures. Moreover, Limited Progress Visibility compounds the predicament, potentially culminating in deferred estimates that amplify the toll on resources is referred in two publications [60, 63]. This dual challenge underscores the profound ramifications of inadequate documentation practices within the RPA landscape. Perceiving RPA as an IT Project, present in one publication, denotes that viewing RPA solely as an IT project introduces the risk of siloed implementation [65]. This limited perspective may hinder organizational-wide optimization and collaboration, posing a risk to business continuity. A broader, business-centric view of RPA is essential to mitigate this risk and ensure seamless integration across departments.

Furthermore, the General Lack of Oversight of Risk, is highlighted in four publications [66–69]. A general lack of oversight introduces risks related to unidentified and unmanaged challenges. Unexpected problems may surface, impacting business operations and continuity. A robust risk management framework, including proactive monitoring and mitigation strategies, is essential to address this risk and maintain business continuity. Selection of Inappropriate Advisors or Partners is notably present in ten publications [60, 62, 66, 70–76]. The consistent emphasis on the selection of advisors or partners as a challenge highlights the significant risk associated with an erroneous sourcing model. Choosing the wrong consulting partner or lacking internal skills may result in extensive damage to business continuity. Informed decision-making and due diligence in partner selection are crucial to mitigating this risk. Unrealistic Expectations is present in nine publications [60, 62, 65, 72, 74, 77–80]. Unrealistic expectations pose risks to the successful integration of RPA into business operations. Overestimating the capabilities of RPA or expecting an immediate optimal return on investment (ROI) may lead to disappointment and disrupt ongoing business processes. Realistic goal-setting and transparent communication are essential to mitigate this risk and maintain business continuity.

Isolated/One-off Goals is outlined in seven publications [61–63, 71, 78, 81, 82]. Focusing on isolated or one-off goals introduces risks to overall business strategy and continuity. Independent automation islands may lead to disruptions and decreased quality in business processes. A cohesive, organization-wide approach to RPA implementation is vital to mitigate this risk and ensure sustained business continuity. The ROI-Driven Change perspective, present in 4 Publications, denotes that implementing RPA solely based on ROI considerations introduces risks to broader business objectives and continuity [63, 75, 83, 84]. Focusing narrowly on financial outcomes may overlook other critical impacts on operations. Considering both financial and operational aspects, a balanced approach is necessary to mitigate this risk and ensure

holistic business continuity. High Implementation Costs, pointed out in six publications, emphasize that the high costs associated with RPA implementation introduce financial risks that may impact business continuity [80, 85–89]. Particularly for smaller organizations with constrained budgets, the challenge lies in justifying the expenses versus the anticipated benefits. Effective cost-benefit analysis and financial planning are essential to mitigate this risk and ensure the sustainability of RPA initiatives. Table 4 outlines the risk factors identified through the study, accompanied by citations of the authors who have discussed these risks.

Table 4 - Risk Factors associated with Management: Major findings and corresponding references.

Category	Risk Factors found	References
Management	MG01 – Inadequate documentation	[52, 60–98]
	MG02 – Lack of visible progress and results	
	MG03 – View RPA as an IT project, not a business initiative	
	MG04 – RPA implementations exceeding typical deployment timelines.	
	MG05 – Very expensive implementation	
	MG06 – Costly maintenance	
	MG07 – Reputational damage	
	MG08 – Not optimizing processes before automating them	
	MG09 – Inefficient implementation of RPA	
	MG10 – Senior IT roles may become overburdened	
	MG11 – Drive change only by ROI perspective	
	MG12 – Unrealistic expectations	
	MG13 – Fail to develop a solid business case for RPA	
	MG14 – Isolated/one off goals	
	MG15 – General lack of oversight of risk	
	MG16 – Pick wrong advisors/partners or pick right advisors too late	

Furthermore, Expensive Maintenance, appears in seven publications, indicating that the evolving nature of RPA and the associated training costs introduce risks to ongoing business operations [62, 66, 69–71, 85, 88]. Inadequate adaptation to these changes may lead to skill gaps and hinder business continuity. Proactive training programs and strategic workforce planning are crucial to mitigating this risk and ensuring continuous RPA functionality. Failure to Develop a Solid Business Case is present in two publications [65, 83]. A lack of a solid business case introduces risks to the alignment of RPA initiatives with organizational goals. Without a clear understanding of business priorities, the risk of misdirected efforts and disrupted business continuity increases. Thorough business case development and strategic planning are crucial to mitigate this risk. Increased Burden on Senior IT Roles is present in one publication [85]. The elimination of operational roles may strain senior IT roles, posing risks to workforce management and business continuity. Overburdened senior IT managers may face challenges in adapting to new responsibilities. Strategic workforce planning and role realignment are crucial to mitigating this risk and ensuring smooth business continuity.

Additionally, Inadequate Process Optimization addressed in seven publications introduces operational risks, impacting the efficiency of RPA implementations. The risk lies in automating suboptimal processes, leading to disruptions in business operations. A comprehensive process optimization strategy is vital to mitigate this risk and enhance overall business continuity. Inefficient RPA implementations, present in eight publications, materialize as an unfortunate corollary, resonating a discordant note in the work of automation [61, 64, 66, 69, 90, 95, 97, 98]. At the same time, a lack of risk vigilance, coupled with expectations and an exclusive pursuit of ROI, compounds the morass of suboptimal outcomes. These multifaceted challenges collectively accentuate the exigency for meticulous strategic planning, interdisciplinary collaboration, and a clever approach to RPA implementation. Applying Traditional Software Delivery Methods present in one publication intends to denote that employing traditional software delivery methods may impede the agility required for business continuity [65, 90]. The risk lies in extended deployment timelines, potentially delaying the realization of RPA benefits. Embracing continuous software delivery practices is critical to mitigate this risk and maintain a dynamic and responsive RPA framework.

Likewise, Reputational Damage is outlined in three publications [87, 90, 91]. Reputational risks emerge when RPA decisions result in biased outcomes or ethically questionable decisions. The potential

damage to an organization's reputation poses a risk to business continuity, affecting stakeholder trust and relationships. Implementing ethical guidelines and robust controls is imperative to mitigate this risk and safeguard business continuity.

Operational Risk Factors

From an operational standpoint, navigating the challenges associated with implementing and utilising Robotic Process Automation (RPA) requires not only an acknowledgment of these obstacles but also a nuanced analysis to inform strategic decision-making. The identified challenges, extracted from diverse publications, present critical insights into the complexities of RPA integration and underscore the significance of proactive measures. Excessive Automation Ambitions, found in two publications, attempting to automate an extensive array of processes, as highlighted, can prove inefficient [60, 62]. Optimal RPA project initiation involves commencing with simpler processes to accumulate experience gradually, rather than prematurely attempting comprehensive automation. In Table 5, we compile identified operational risk factors, duly referenced to their respective authors, shedding light on the nuanced challenges inherent in RPA integration.

Additionally, the Underutilization of Bots, as discussed in three publications, the overconfidence stemming from the maturity of RPA projects may lead to the underutilization of bots, diminishing their effectiveness and profitability [60, 62, 99]. Organizations must strike a balance in leveraging bots to ensure optimal outcomes from their deployment. Insufficient Robot Deployment, mentioned in two publications, inadequate deployment of robots may result in partially automated processes, rendering them error-prone [60, 62]. Moreover, widespread shortages of bots could impede seamless operations, highlighting the need for comprehensive automation coverage.

Table 5 – Findings related to Operational Risk Factors and their references.

Category	Risk Factors found	References
Operational	OP01 – Try to automate too much	[52, 60, 62, 63, 65–67, 70–72, 78, 81, 82, 84, 86, 87, 94, 99–112]
	OP02 – Underutilization of bots	
	OP03 – Not enough robots	
	OP04 – Incorrect process selection	
	OP05 – IT not involved/uncooperative	
	OP06 – Selecting the wrong tool	
	OP07 – Lack of segregation of RPA development and production	
	OP08 – Challenges in identifying sustainable automation use cases	
	OP09 – Inconsistent and insecure bot development and management	
	OP10 – Lack of strategic intent	
	OP11 – Poor strategic reputation	
	OP12 – Contractual risks	

Additionally, the Erroneous Process Selection, highlighted in nine publications, the selection of inappropriate processes for automation, extensively discussed, poses a significant risk [66, 71, 81, 84, 100, 102, 105, 111, 112]. Applying RPA to complex and costly processes with limited returns can jeopardize the success of the automation initiative. IT Involvement Challenges, emphasized in three publications, the absence of collaboration or cooperation from the IT department, as emphasized, presents a notable risk [60, 62, 63]. Stakeholders initiating RPA without IT consent or IT departments unwilling to participate hinder the success of RPA implementation.

Furthermore, Tool Selection Challenges, addressed in eight publications, the challenge of selecting the right automation tool, extensively addressed, arises due to the abundance of options in the market [60, 62, 66, 70, 87, 101, 109, 110]. Incorrect tool choices can lead to errors, emphasizing the need to carefully evaluate tools aligned with specific business processes. Segregation of RPA Development and Production, highlighted in three publications, may lead to inadequate segregation of RPA development and production, a concern raised, that hampers flexibility and change implementation [63, 66, 67]. Proper modularization is essential for facilitating changes and ensuring seamless transitions to production. The Identification of

Use Cases, noted in three publications, difficulty in identifying suitable use cases, as noted, can impede the creation of a robust automation pipeline [65, 71, 72]. A detailed understanding of business processes is vital for realizing the expected performance improvements through RPA.

Moreover, Inconsistent Bot Development and Management, outlined in three publications, and the lack of consistent and secure development and management of bots, outlined, introduces challenges [64, 67, 104]. Effective management, maintenance, and security measures are essential to mitigate IT overhead and ensure the solidity of the RPA implementation. The Lack of Strategic Intent, explored in eleven publications, explored extensively, the lack of strategic intent signifies a miscalculation in selecting processes for unassisted versus assisted RPA [65, 82] [62, 65], [82] [62, 63, 65, 78] [103]. It may result from a narrow focus on cost reduction without a broader digital transformation strategy, necessitating careful planning and assessment.

Likewise, Poor Strategic Reputation, addressed in two publications, poor strategic reputation, addressed, results from inadequacies in the implementation strategy, tarnishing the internal and external perception of RPA service providers and the organization itself [60, 62]. Contractual Risks, discussed in one publication, denote that the innovation surge in the RPA sector introduces contractual risks, particularly with smaller providers [73]. Organizations need to assess providers' capacity and financial strength to manage these contractual risks effectively.

Governance Risk Factors

From a governance perspective, several critical challenges in the implementation of RPA come to light. One primary issue is the oversight in establishing a change management capability, an aspect underscored in three publications [66, 113]. Implementing RPA necessitates the creation of a framework enabling subsequent modifications to processes. This ensures robust and consistent application maintenance without disrupting the established workflow. Table 6 provides an overview of Governance-related risk factors identified in the research, accompanied by corresponding author references.

Table 6 – Key Governance Risk Factors perspectives and their references.

Category	Risk Factors found	References
Governance	GV01 – Not building change management capability	[52, 60–63, 66–69, 71, 77, 80–85, 87–92, 95, 104, 105, 107, 111, 113–118]
	GV02 – General lack of controls	
	GV03 – No component reusability	
	GV04 – Insufficient record-keeping	
	GV05 – Very expensive implementation	
	GV06 – Unclear roles	
	GV07 – Employee resistance to change	
	GV08 – Neglecting algorithm and data source monitoring for RPA.	
	GV09 – No formal process for assessing bot impact on source app changes.	
	GV10 – No formal process for requesting and implementing bot changes.	
	GV11 – Poor governance of RPA	
	GV12 – Lack of communication plan	

In addition, the absence of component reusability, mentioned in one publication, signifies an overlooked opportunity[63]. When planning RPA initiatives, the consideration of implementing transversal modules allows for the future utilization of these components in new process implementations. This conserves time and resources and amplifies the efficiency of RPA applications [89, 116].

Furthermore, a general deficiency in controls, as noted in four publications, emerges as a significant concern [66, 67, 92, 104]. Over time, it is natural to question the efficacy of RPA bots. This query may signal a dearth of automated alerting tools for error handling. Continuous monitoring, even post-successful implementation, is imperative to mitigate the potential adverse impacts of bot failures on organisational operations [71, 104].

Another critical aspect pertains to poor record-keeping practices, an issue elaborated upon in three publications [63, 64, 87]. This deficiency can lead to suboptimal implementation design, thereby catalysing challenges in execution and maintenance [106]. Furthermore, it hampers process reusability, highlighting the pivotal role of comprehensive documentation in the effective deployment of RPA [80][104].

The matter of excessive implementation costs surfaces prominently, with six publications discussing the financial constraints associated with RPA adoption [80, 85, 87–89, 115]. While RPA holds significant potential for productivity enhancements, its cost-prohibitive nature may pose challenges for certain organisations, particularly smaller entities or those grappling with cash flow limitations [114]. The expense associated with customization and implementation, especially for complex tasks requiring nuanced judgment or creativity, warrants careful consideration in the evaluation of RPA feasibility [85, 89]. Additionally, the unanticipated costs and prolonged timelines associated with implementing many bots may necessitate a re-evaluation of organisational expectations [80, 118][106].

Technology Risk Factors

From a technological standpoint, several critical challenges impede the effective integration of RPA within organisational frameworks [52]. A recurring concern, discussed in seven publications, centers on the reluctance to embrace new technologies as RPA initiatives mature [60–63, 68, 78, 97]. This resistance stems from a desire to avoid altering established processes, potentially entrenching legacy practices over time. Furthermore, five publications highlight the predicament of legacy application silos [63, 71, 78, 97, 117]. Outdated applications are susceptible to processing errors and may not adequately support RPA execution, thereby rendering them unsuitable for automation initiatives. Additionally, the waning support for legacy applications exacerbates the risk, potentially necessitating costly upgrades and subsequent modifications to existing RPA implementations [69, 102]. Table 7 furnishes a summary of the Technology-associated risk factors elucidated in the study, accompanied by respective author citations.

Table 7 - List of critical Technology Risk Factors and their references.

Category	Risk Factors found	References
Technology	TC01 – Lack of integration with new technologies	[52, 60–63, 65, 66, 68, 69, 71, 78, 83, 87, 90–92, 94, 95, 97, 99, 101, 102, 110–112, 117, 119–128]
	TC02 – Legacy apps silos	
	TC03 – No component reusability	
	TC04 – Lack of standardization	
	TC05 – Robot malfunctions or operational deviations due to technical issues	
	TC06 – Lack of scalability	
	TC07 – Exception handling	
	TC08 – Lack of integration with new technologies	
	TC09 – Poor design	
	TC10 – Neglects planning for scalable and secure RPA infrastructure	
	TC11 – Lack of integration with new technologies	

Another pivotal issue pertains to the reusability of RPA components, a consideration expounded in a single publication. When conceptualizing an RPA project, the strategic incorporation of cross-functional modules offers a transformative potential. These modules can be repurposed for new process implementations, yielding substantial time and cost savings by leveraging previously developed components [60, 71, 97, 117].

The inadequacy of standardization is a salient challenge, as articulated in two publications [65, 69]. This deficiency in well-defined rules and process standardization thwarts the potential for cross-process reuse, thereby incurring additional expenditures of time and resources. Additionally, technical issues emerge as a prevalent concern, emphasized in twenty publications [61, 62, 66, 69, 70, 83, 87, 90–92, 94, 95, 101, 102, 110–112, 119, 121, 122]. When RPA operations deviate from their intended course, the ramifications permeate the entire business process and dataset. Failures may arise from a variety of sources, including changes in the underlying applications or unanticipated deviations in business processes.

Scalability issues, noted in five publications, pose a considerable hurdle for organisations seeking to expand their RPA initiatives [63, 121, 123–125]. While RPA bots are relatively straightforward to implement, complexity in their governance and management can impede seamless scaling. Exception handling presents another critical consideration, addressed in eight publications [61, 64, 68, 87, 99, 117, 126, 127]. This entails managing two distinct types of exceptions: Business Exceptions, which pertain to previously defined processes or unanticipated dependencies, and Application/System Exceptions,

encompassing scenarios where bots encounter obstacles in connecting to external applications or face permission-related constraints.

Moreover, five publications underscore the imperative of robust bot design [66, 69, 87, 120, 128]. A poorly designed RPA bot may inadvertently expose sensitive information, ranging from personal data to financial records, particularly when execution occurs on public networks. Finally, a lack of foresight in delineating the requisite IT infrastructure for scaling and safeguarding RPA processes emerges as a concern noted in two publications. This issue arises when outsourcing consultancies fail to establish a robust foundation for automation, hindering the seamless extension of automation to related processes.

Security Risk Factors

From a security standpoint, numerous critical considerations arise in the integration of RPA within organisational frameworks. Network vulnerability, an issue addressed in thirteen publications, poses a significant threat [66, 70, 73, 78, 86, 90, 95, 111, 117, 120, 129–131]. The compromise of an organisation's network infrastructure can directly impact the seamless execution of RPA bots. For instance, a software update crucial to bot operations necessitates a stable network connection. If this connection is plagued by recurrent failures, it jeopardizes the successful execution of RPA tasks. Table 8 offers a succinct summary of security-related risk factors identified in the research, complete with corresponding author references.

Table 8 - Risk Factors associated with Security: Key findings and their references.

Category	Risk Factors found	References
Security	SC01 – Network vulnerability	[52, 63, 65–67, 69, 70, 73, 81, 84–86, 90, 95, 101, 109, 111, 117, 120, 124, 126, 128–135]
	SC02 – Denial-of-service interruptions	
	SC03 – Remote code execution	
	SC04 – Inappropriate access to sensitive data	
	SC05 – Abuse of administration privileges	
	SC06 – Lack of access management	
	SC07 – Data leakage	
	SC08 – Fraud	

Denial-of-service interruptions, emphasized in three publications, represent another significant challenge [66, 70, 129]. Multiple bots' rapid and simultaneous activation can overwhelm the network, leading to service disruptions. This, in turn, can pave the way for potential security breaches. Furthermore, remote code execution, mentioned in one publication, demands meticulous attention to security protocols [93]. Ensuring robust encryption of data and bolstering network and cloud protection mechanisms are imperative to mitigate compliance risks that could compromise the execution of RPA bot code.

Inappropriate access to sensitive data, a concern discussed in eleven publications, underscores the importance of proper bot configuration [65, 67, 70, 84, 93, 111, 120, 126, 129, 132, 133]. Mishandled access privileges can result in unauthorized entry to sensitive information, potentially triggering compliance conflicts within the organisation. Additionally, the scenario may arise where a bot requires access to sensitive data to fulfil its tasks, providing an opportunity for unscrupulous employees to exploit this misconfiguration for personal gain.

The abuse of administrative privileges, outlined in eight publications, introduces a multifaceted security challenge [65, 66, 70, 78, 120, 129, 132, 133]. Administrators may misuse their elevated access levels to gain unauthorized entry to sensitive processes or data. This can manifest as the unauthorized extraction or even sale of sensitive information to external entities. Alternatively, administrators may improperly grant access to select employees, conferring them an unfair advantage within the organisation.

Furthermore, the lack of bot accountability pertaining to security, privacy, and compliance requirements, a concern discussed in five publications, is of paramount significance [66, 67, 95, 117, 129]. Bots must uphold their role in compliance with security protocols. The absence of such accountability can impede the identification of vulnerabilities within the organisation, complicating efforts to trace the origin of security breaches.

Resources Risk Factors

From a resource's perspective, several critical challenges emerge in the integration of RPA within organisational workflows. Employee resistance to change, as highlighted in five publications, constitutes a significant hurdle [63, 69, 83, 84, 118]. Rapid process alterations can lead to operational disruptions, causing the related bots to malfunction and generate a plethora of exceptions. This inadvertently reverses the anticipated reduction in the workforce, resulting in heightened workloads and employee discontent. Such circumstances may breed reluctance among employees to re-engage with RPA processes, impeding the smooth operation of automation initiatives.

Human error, identified in five publications, presents a pervasive risk [63, 64, 113, 122, 136]. Various forms of human oversight can occur, exemplified by developer mistakes during the configuration phase. For instance, misdirecting the bot to retrieve data from an incorrect source can lead to subsequent data manipulation errors. This error could propagate swiftly through the organisation if undetected during testing, potentially corrupting critical data sets. Table 9 gives a compact overview of Resource-related risk factors outlined in the research, including references to the respective authors.

Table 9 - Risk Factors related to Resources and their reference sources.

Category	Risk Factors found	References
Resources	RS01 – Employee resistance to change	[52, 60–63, 65–67, 69, 75, 78, 83, 84, 100, 101, 107, 109, 113, 118, 122, 130, 136–142]
	RS02 – Human error	
	RS03 – Lack of experienced RPA resources	
	RS04 – Lack of user know-how	
	RS05 – Underestimating human capital,	
	RS06 – Skills leakage/shortage	
	RS07 – Under-resourcing your RPA projects	
	RS08 – Reduce expertise	

The need of experienced RPA resources, discussed in six publications, underscores a pressing concern [63, 65, 78, 101, 109, 140]. Given the novelty of RPA technology, finding candidates with the requisite skills and expertise can be challenging. This can compel stakeholders to onboard individuals lacking the necessary proficiency to handle RPA implementations' intricacies. Additionally, a deficiency in user proficiency, noted in fourteen publications, raises a pivotal consideration [60, 62, 63, 66, 75, 100, 107, 109, 118, 130, 137, 138, 141, 142]. Employees may harbour apprehensions about automation displacing their roles. Moreover, misconceptions or limited understanding of RPA's potential may hinder its acceptance within the organisation, stemming from concerns about job security and labour market dynamics.

Underestimating the significance of human capital in RPA implementation, as cited in two publications, can lead to project failure [60, 65]. Engaging the IT department is crucial for large-scale RPA activities, as it provides the requisite knowledge and infrastructure for bot maintenance and adjustments. Skills leakage and shortage, detailed in eight publications, pose a substantial risk [60, 62, 65–67, 78, 109, 139]. Assuming that rudimentary user skills suffice for deploying RPA in production can be perilous. Effective decision-making in automation demands continuous learning, particularly in testing processes, to ensure optimal outcomes.

Moreover, under-resourcing RPA projects, as mentioned in three publications, may result from the aforementioned risks [60–62]. Insufficiently defined objectives can compel organisations to outsource RPA initiatives for suboptimal reasons. Finally, the risk of reduced expertise, as acknowledged in one publication, arises from automating decision processes without due consideration for potential missed opportunities [60]. This can inadvertently create an environment where outcomes are unquestioningly determined by historical behaviour, potentially leading to suboptimal results.

Business Continuity Risk Factors

From a business continuity perspective, several critical risk factors necessitate careful consideration in the integration of RPA within organisational workflows. Regulatory risk, as elucidated in six publications, emerges as a prominent concern [66, 69, 73, 78, 87, 143]. The dynamic nature of laws and regulations mandates continuous monitoring and adaptation of RPA bots to align with evolving government mandates. Failing to update these bots can expose an organisation to regulatory liabilities. Moreover, utilizing

inadequately tested or invalid algorithms in bot operations can lead to financial losses, compromising the integrity and accuracy of financial reporting, and potentially resulting in improper transaction recording or delayed payments. The absence of standardized regulatory frameworks for automated bots exacerbates this risk, leaving organisations vulnerable to inadvertent legal violations[32, 33].

Compliance risks, outlined in eleven publications, warrant diligent attention in the context of RPA implementation [60, 62, 66, 87, 90, 96, 103, 113, 117, 128, 144]. Neglecting to incorporate robust compliance processes into RPA development can lead to non-compliance with critical business requirements and Key Performance Indicators (KPIs). Inadequate explanation of RPA-generated results to regulatory authorities may result in penalties or, in severe cases, the revocation of operating licenses. For instance, consider a scenario where a marketing team initiates RPA-driven data collection for targeted marketing campaigns. Failing to secure proper parental consent for the collection of minors' data could introduce a significant compliance risk.

Table 10 - Critical Business Continuity Risk Factors in RPA Integration with Author References

Category	Risk Factors found	References
Business Continuity	BC01 – Compliance risks	[60–62, 66, 67, 69, 73, 78, 81, 82, 84, 87, 90, 93, 95–97, 101, 103, 111, 113, 117, 126, 128, 129, 131, 132, 143–146]
	BC02 – Regulatory risk	
	BC03 – Lack of Business continuity preparedness	
	BC04 – Failing to Map Dependencies	
	BC05 – External threats	
	BC06 – Internal threats	
	BC07 – Insufficient bot accountability for security, privacy, and compliance	

Mapping dependencies, highlighted in two publications, is a critical aspect often overlooked [81, 97]. A common failure point arises when bots cease to function due to changes in the user interface with which the automated process interacts. Inadequate mapping of technical and functional dependencies between RPA bots and other systems can lead to project failure. Thoroughly understanding and documenting these dependencies is crucial for seamless bot operation. Table 10 provides a concise summary of Business Continuity-related risk factors delineated in the research and corresponding author references.

External threats, as identified in fourteen publications, present a formidable risk in the RPA landscape [66, 78, 84, 87, 93, 95, 101, 103, 111, 126, 132, 136, 145, 146]. Inadequate bot security can leave an organisation vulnerable to hackers seeking unauthorized access to confidential data. Regular security testing and risk assessments are imperative to safeguard against potential breaches. Additionally, there exists a concerning scenario where a malicious actor could compromise an organisation's own RPA bot to extract sensitive data or hold it ransom for extortionate sums.

Internal threats, discussed in six publications, underscore the potential risks originating from within the organisation itself [66, 78, 84, 90, 131, 145]. Instances may occur where an internal employee manipulates or reprograms a bot for nefarious purposes, leading to data breaches or unauthorized access. For instance, a former employee could exploit RPA capabilities to illicitly extract customer relationship data, potentially resulting in significant security breaches. Establishing unified, secure, and efficient Identity and Access Management (IAM) practices is imperative to mitigate this internal threat.

Data Risk Factors

Insufficiently secured data management, discussed in nine publications, arises when a bot handles sensitive information without encrypting it prior to transmission to a cloud environment [66, 78, 90, 92, 95, 101, 120, 126, 146]. This oversight exposes the data to potential interception or decryption by unauthorized parties. For instance, an incident occurred in a banking context where customers received statements belonging to other individuals via email. Upon investigation, it was determined that an RPA bot was responsible for the erroneous distribution. This inadvertent disclosure of confidential information underscores the importance of secure data management in RPA operations. Table 13 presents Data-related risk factors from the research, accompanied by references from the authors.

Unauthorized access to confidential information, emphasized in eleven publications, can result from the misconfiguration of a bot, leading to improper access and potential compliance conflicts within the

organisation [65, 67, 70, 84, 93, 111, 120, 126, 129, 132, 133]. Moreover, there exists a scenario where a bot, necessitating access to sensitive data for task completion, may be exploited by an employee for personal gain or unauthorized viewing. Data leakage, a concern articulated in nine publications, presents a risk where sensitive data, including credentials or customer information, could be exposed to external threats in the absence of adequate security measures [78, 102, 129, 131, 132, 134, 145, 147, 148]. This vulnerability may enable malicious actors to illicitly extract data from the organisation.

Table 11 - Data Risk Factors in RPA Operations and Reference Sources

Category	Risk Factors found	References
Data	DT01 – Unauthorized access to confidential information	[63, 65–67, 70, 77, 83, 84, 90, 92, 93, 95, 101, 102, 111, 116, 117, 120, 126, 129, 131–134, 145–150]
	DT02 – Unsecure data management	
	DT03 – Data leakage	
	DT04 – Bad quality of data	

Inadequate or bad data quality, a topic covered in seven publications, represents a noteworthy challenge for RPA implementation [63, 66, 77, 83, 116, 117, 149]. RPA systems are optimized for structured data; operational issues may arise if data quality is subpar. Unlike humans, RPA bots may not readily discern glaring data errors, potentially propagating and amplifying inaccuracies that could have been readily identified by a human observer.

5 Results and Discussion

The primary objective of this research is to delineate the principal risks inherent in the utilization and implementation of RPA. They have been categorised to systematically organize these risks, as illustrated in Figure 8. The meticulous grouping of these risk factors affords a nuanced comprehension of their strategic positioning and potential ramifications on RPA implementation. This categorization enables a more comprehensive vision of the alignment of each risk factor, elucidating their collective impact on the landscape of business continuity [1]. Additionally, this categorization aids in comprehending how these risks influence various facets of organizational operations [3]. The extraction of insights from grey and academic literature further facilitates an understanding of the primary domains in which these risks may exert influence [59].

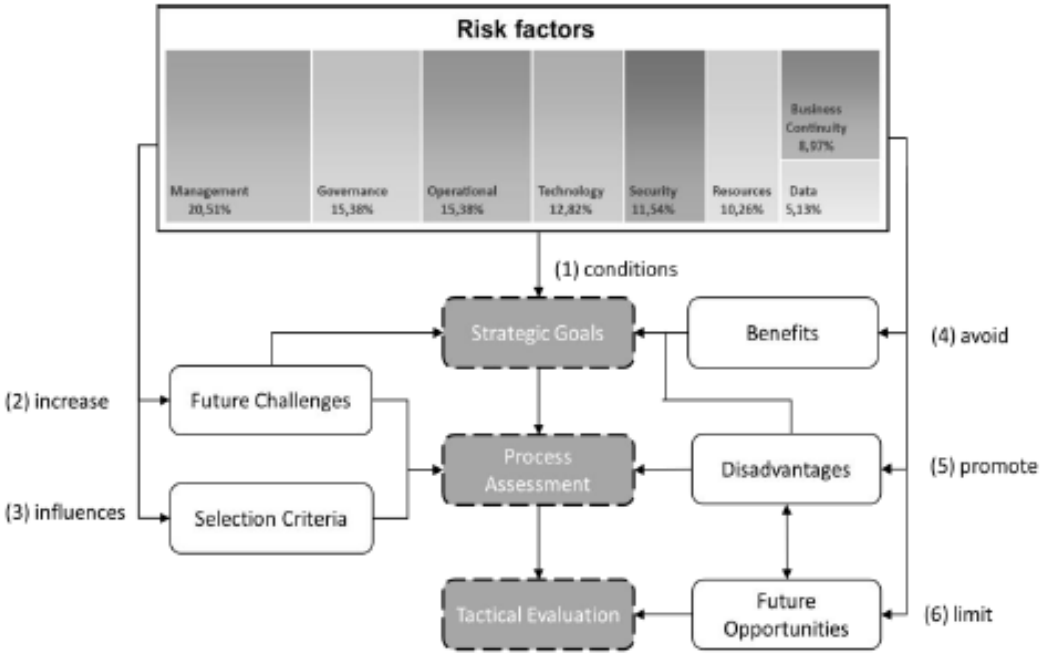


Fig. 8 – Merge of Risk Factors with the main concepts around RPA implementation and their relationships

In the context of implementing RPA within an organisation, various risk factors play a pivotal role in shaping the outcomes of the process. These risk factors can be classified into distinct categories based on their influence and are expressed in Figure 8 in terms of relationships, expressed in arrows (1) to (6), that can impact the implementation of RPA in organisations.

1) Categorization and Strategic Relationships

Figure 8 serves as a dynamic canvas, portraying the categorization of risk factors and the intricate relationships between them. The arrows (1) to (6) act as conduits, delineating critical linkages that profoundly influence the trajectory of RPA integration within organizations:

Conditions of Favourable Outcomes (1): In contrast to the paradigm of guiding organizations toward favourable outcomes, certain identified risk factors emerge as conditioning agents within the RPA implementation landscape. Rather than facilitating a trajectory towards advantageous conditions, these factors impose constraints and contingencies that necessitate careful consideration. This nuanced perspective reframes the discourse, emphasizing that proactive mitigation is imperative not merely to guide the implementation but, more crucially, to manage and navigate the imposed conditions effectively. In essence, it underscores the strategic imperative of addressing and conditioning these factors to ensure that the RPA implementation aligns with and optimally serves strategic goals [25]. This alternative interpretation adds depth to the narrative, recognizing certain risk factors' dual nature as guiding and conditioning forces within the intricate tapestry of RPA integration.

Exacerbation of Challenges (2): Arrow 2, symbolizing the exacerbation of challenges within the RPA implementation landscape, denotes a nuanced revelation that augments our comprehension of the intricacies involved. This arrow signifies the potential compounding effect of certain risk factors, magnifying existing challenges and introducing a layer of complexity that demands careful consideration. The identification of risk factors as exacerbators (2) underscores their role in intensifying hurdles encountered during the implementation journey [19]. This exacerbation goes beyond the mere presence of challenges, suggesting that specific risk factors possess the capacity to act as catalysts, amplifying the impact and intricacy of pre-existing difficulties. This insight prompts a re-evaluation of risk management strategies, emphasizing the necessity for organizations to recognise challenges and the specific risk factors contributing to their exacerbation. Arrow 2 signals a clarion call for strategic foresight, urging organizations to proactively address these exacerbating factors. Without such targeted mitigation efforts, there is a heightened risk of challenges compounding, leading to a more intricate and formidable terrain for RPA implementation. Arrow 2 serves as a pivotal indicator, urging organizations to delve into the granular details of identified risk factors, understand their potential compounding effects on challenges, and strategically tailor mitigation approaches. This proactive stance is essential for organizations seeking not only to navigate challenges but to do so with a keen awareness of the factors that may intensify their impact [1].

Influence on Decision Criteria (3): Recognizing the influence of risk factors on decision criteria (arrow 3) becomes a fundamental element for informed decision-making. This understanding empowers organizations to align their strategic goals, process assessment, and tactical evaluation with the identified risk factors. This arrow accentuates the nuanced interplay between identified risk factors and the criteria shaping strategic goals, process assessment, and tactical evaluation. In the realm of business continuity, where decision-making holds profound implications for organizational resilience, recognizing the influence of risk factors on decision criteria becomes paramount. This recognition stands as a fundamental tenet, empowering organizations to elevate their decision-making processes beyond routine considerations to align with the exigencies of business continuity. Understanding this influence (3) becomes a key element for organizations seeking to fortify their business continuity strategies. It prompts a strategic re-evaluation of decision criteria, fortified with a keen awareness of how risk factors may impact the overarching goals of business continuity in RPA implementation. By acknowledging and incorporating the influence of risk factors on decision criteria, organizations gain a distinct advantage in aligning their strategic goals, refining their process assessment, and enhancing tactical evaluation. This strategic alignment is vital for ensuring that decision-making processes address immediate challenges and embed a proactive orientation toward maintaining business continuity amidst potential disruptions. Arrow 3, within the context of business

continuity, underscores the imperative for organizations to introduce resilience into their decision-making frameworks. It advocates for a comprehensive understanding of how risk factors can shape decision criteria, thereby empowering organizations to make informed choices that resonate with the imperatives of business continuity in the dynamic landscape of RPA implementation [3, 28].

Degrading Benefits Realization (4): Arrow 4, symbolizing the degradation of benefits realization within the purview of business continuity in RPA implementation, unveils a critical dimension that demands meticulous consideration. This arrow accentuates the propensity of certain risk factors to serve as catalysts, impeding the attainment of benefits associated with strategic goals and the overarching implementation process. Some risk factors act as catalysts, hindering the realization of benefits associated with strategic goals and the broader implementation process. Unveiling these factors becomes crucial in ensuring positive outcomes and optimizing the RPA implementation. Identifying these catalysts (4) becomes an indispensable step in ensuring positive outcomes and optimizing the RPA implementation for business continuity [19]. It prompts organizations to scrutinize the intricate interplay between identified risk factors and the envisaged benefits, fostering a proactive stance in mitigating impediments to the realization of strategic goals. In the realm of business continuity, where seamless operations and resilience are paramount, Arrow 4 calls for an intensified focus on strategic planning and risk mitigation. Unveiling the specific risk factors that impede benefits realization is pivotal for organizations to fortify their continuity strategies. By doing so, organizations can safeguard against potential disruptions, optimize their RPA implementation for resilience, and ensure that the anticipated benefits are not only realized but sustained in the face of potential challenges. This insight, rooted in business continuity considerations, underscores the strategic imperative of addressing these catalysts to fortify the benefits realization framework within the RPA implementation spectrum [1].

Escalation of Difficulties (5): Arrow (5) in Figure 8 becomes emblematic of the consequential trajectory that unfolds in the absence of strategic mitigation measures. It accentuates the propensity for these risk factors to catalyse a cascading effect, amplifying difficulties across the entire implementation spectrum. This cascade, if left unchecked, has the potential to impede and even stall the overall progress of the RPA initiative. The significance of this revelation lies in its call to action. It underscores the imperative for organizations to not only identify and understand these exacerbating risk factors but, more critically, to proactively implement strategic mitigation measures. Without such foresighted intervention, the increasing challenges have the propensity to snowball into formidable impediments, hindering the intended progression of the RPA implementation journey. This insight prompts a strategic re-evaluation of risk management frameworks, emphasizing the need for anticipatory measures that extend beyond mere identification. Organizations are urged to delve into the proactive formulation of mitigation strategies tailored to address the specific nature of these exacerbating risk factors. By doing so, they fortify their resilience against the potential escalation of difficulties, thus safeguarding the fluidity and effectiveness of the RPA implementation process [14, 34].

Influence on Future Opportunities (6): Beyond immediate challenges, risk factors can also influence future opportunities (arrow 6). By recognizing and addressing these factors, organizations position themselves strategically to capitalize on emerging possibilities. In the realm of business continuity, the capacity of risk factors to influence future opportunities becomes a strategic consideration of paramount importance. The recognition and proactive addressing of these factors are pivotal steps for organizations aiming to position themselves strategically in anticipation of evolving scenarios. This insight prompts organizations to view risk factors not merely as impediments but as dynamic variables that can frame the future trajectory of their business continuity strategies. By discerning and addressing these factors, organizations fortify their resilience against immediate challenges and position themselves strategically to capitalize on emerging possibilities. In the context of business continuity, where adaptability and foresight are central tenets, Arrow 6 signifies the imperative for organizations to go beyond reactive risk management. Instead, they are encouraged to adopt a proactive stance that mitigates current challenges and strategically aligns with the evolving landscape, enabling them to seize future opportunities. By addressing risk factors that influence future opportunities, organizations augment their preparedness for contingencies, cultivate adaptability in the face of change, and position themselves as proactive architects of their business continuity landscape. This strategic orientation enables them not only to navigate challenges but also to

harness emerging possibilities, thereby fostering a resilient and forward-looking approach in the realm of RPA implementation and business continuity [34].

2) Key insights:

Categorization and Understanding of Risks: The overview reveals a meticulous categorization of principal risks associated with the implementation of RPA. This categorization enhances our understanding of the multifaceted challenges that organizations may encounter during RPA integration [59].

Strategic Relationships and Impact: The depiction of arrows (1) to (6) in Figure 8 highlights the strategic relationships between different risk factors. This insight elucidates how these risks are interconnected and can influence each other, offering a dynamic view of their potential impact on the implementation of RPA within organizations [26].

Guidance Toward Favourable Outcomes: Certain risk factors possess the potential to guide organizations toward favourable conditions. This understanding emphasizes the importance of proactive mitigation strategies to steer RPA implementation in a direction aligned with strategic goals and positive outcomes [28].

Recognition of Catalysts and Challenges: The identification of risk factors acting as catalysts or exacerbating challenges underscores the need for targeted mitigation efforts. Addressing these factors becomes crucial to prevent an escalation of difficulties, ensuring smoother progress in RPA implementation [5].

Influence on Decision-Making Criteria: The insight into how risk factors influence decision criteria (arrow 3) emphasizes the importance of informed decision-making throughout the implementation process. Recognizing these influences enables organizations to align their strategic goals, process assessment, and tactical evaluation with identified risk factors [4].

Synthesis of Insights and New Comprehensive Strategy: The presented approach synthesizes insights from prior research (Figure 1) with current findings to forge a new, comprehensive strategy (Figure 8). This integration addresses existing limitations and provides a strategic foundation for decision-making in the RPA implementation process [151, 152].

Potential for Future Opportunities: The overview suggests that addressing risk factors mitigates challenges and positions organizations strategically to pursue future opportunities (arrow 6). This forward-looking perspective encourages organizations to leverage insights for future growth and adaptability [25].

In summary, understanding the nuanced interactions between risk factors and the various stages of RPA implementation is crucial for effectively managing risks and optimizing outcomes. By proactively addressing these factors and integrating the approach outlined in Figure 1 with the findings of this research, expressed in Figure 8, organisations can navigate the implementation process with greater precision and achieve more favourable results.

6 Conclusions

This study has delved into the complex landscape of risk factors associated with the implementation of RPA within organisational contexts and Business Continuity. Through a comprehensive analysis of research papers and grey literature, we have identified key risk categories, including Management, Governance, Operational, Technology, Security, Resources, Business Continuity, and Data, answering research question 1. These risk factors have been examined in conjunction with three critical steps in the implementation process: "Strategic Goals," "Process Assessment," and "Tactical Evaluation".

By synthesizing insights from prior work (as depicted in Figure 1) with the findings of this research, we have proposed an integrated approach that addresses these risk factors, as presented in Figure 8, answering the second research question. This approach provides a holistic framework for organisations to better navigate challenges, promote benefits, and optimize outcomes throughout the RPA implementation journey.

While this study provides valuable insights into RPA implementation risks, it is important to acknowledge its limitations, as the effectiveness of the proposed integrated approach may vary based on specific organisational contexts and industry domains. It is crucial to consider these factors when applying the findings in practical settings.

From the overview and discussions in the article, we learn that Robotic Process Automation (RPA) presents both significant opportunities and challenges for organizations striving to enhance efficiency, reduce costs, and improve service quality. The comprehensive analysis of risk factors associated with RPA implementation, varying from technological to managerial and operational, underscores the necessity for a strategic approach to adopting RPA technologies. This approach should not only address potential risks but also leverage RPA's capabilities to optimize business processes and continuity.

Moving forward, the path is clear: organizations must adopt a multi-faceted strategy that involves rigorous risk assessment, continuous monitoring, and adaptation of RPA solutions to fit their unique operational landscapes. This includes investing in training and development to bridge the skills gap, ensuring robust governance frameworks are in place, and fostering a culture of innovation that can adapt to the evolving RPA technologies. Moreover, future research should focus on longitudinal studies to understand the long-term impacts of RPA, the development of industry-specific best practices, and the exploration of how RPA can be integrated with emerging technologies like AI and machine learning to unlock new efficiencies. In essence, the journey of RPA implementation is ongoing, with each step forward opening new avenues for operational excellence and strategic competitiveness.

To conclude the article and set the stage for future exploration within the realm of RPA and its risk impacts on business continuity, a comprehensive research agenda is proposed to address the complexities and evolving dynamics of RPA implementations.

This agenda encompasses several pivotal areas:

Depth Analysis of Risk Factors: Future research should aim to conduct an in-depth exploration of the specific risk factors associated with RPA, assessing their variable impacts across diverse industries, organizational sizes, and geographical contexts. Quantitative risk assessment models and sophisticated methodologies could be developed to measure these risks accurately.

Longitudinal Research Approaches: Considering the rapid technological advancements in RPA, longitudinal studies are essential. These studies would provide invaluable insights into the long-term sustainability, effectiveness, and evolving challenges of RPA technologies over time.

Cross-Sectoral Comparative Studies: Engaging in comparative analysis across various sectors and organizational frameworks can unearth best practices and refine governance models for RPA implementation. This would facilitate a comprehensive understanding of the strategic deployment of RPA technologies.

Synergy with Emerging Technological Trends: Investigating the integration of RPA with cutting-edge technologies such as AI, blockchain, and the Internet of Things (IoT) could yield robust, innovative automation solutions, enhancing operational efficiencies and creating new value propositions.

Socio-Technical Impact Studies: Future inquiries should delve into the socio-technical dimensions of RPA, exploring the implications for workforce dynamics, skills requirements, and organizational culture. This includes understanding the human element in the automation equation and its impact on employment, training, and job satisfaction.

Regulatory and Ethical Implications: With the digital era steering in sensitive data privacy concerns and complex regulatory requirements, research must also pivot towards the implications of RPA on compliance, ethical considerations, and data security, ensuring that RPA implementations adhere to legal and ethical standards.

Economic Impact Assessments: Conducting rigorous economic and financial analyses to ascertain the cost-benefit ratios of RPA initiatives is crucial. This encompasses evaluating the ROI, cost savings, and the overall impact on organizational efficiency and competitiveness.

Empirical Case Studies and Implementation Frameworks: The development of detailed case studies on RPA deployments - both successful and unsuccessful - will be instrumental in deriving practical insights and frameworks. Such empirical evidence can guide organizations in navigating the complexities of RPA implementation, facilitating smoother transitions and more effective integration into business processes.

By addressing these areas, future research will significantly contribute to the understanding of RPA's strategic role in enhancing business continuity and operational resilience. This detailed research agenda not only highlights the need for continued academic and practical inquiry into RPA but also sets a robust foundation for future studies to build upon, ensuring that the field remains at the forefront of technological innovation and its application in the business world.

In conclusion, this study contributes to a comprehensive understanding of the risk factors associated with RPA implementation and presents an integrated approach to mitigate these challenges. While acknowledging its limitations, we anticipate that this research will serve as a foundation for future efforts in the dynamic field of RPA implementation strategies.

Declarations

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Lok CP (2021) Critical Success Factors for Robotic Process Automation Implementation. 6
2. Kyherõinen T (2018) Implementation of Robotic Process Automation to a Target Process-a Case Study. 75
3. Santos, F., Pereira, R. & Vasconcelos JB (2020) (2020) Towards Robotic Process Automation implementation: An end-to-end perspective
4. Van den Oever B (2020) Method for estimating the impact of Robotic Process Automation implementations on business processes.
5. Stamford C (2022) Gartner Says Worldwide RPA Software Spending to Reach $2.9 Billion in 2022. https://www.gartner.com/en/newsroom/press-releases/2022-08-1-rpa-forecast-2022-2q22-press-release. Accessed 6 Oct 2022
6. roboticbiz (2020) COVID-19: RPA is a lifeline for business continuity. https://roboticsbiz.com/covid-19-rpa-is-a-lifeline-for-business-continuity/. Accessed 5 Sep 2021
7. Afrianty TW, Artatanaya IGLS, Burgess J (2022) Working from home effectiveness during Covid-19: Evidence from university staff in Indonesia. Asia Pacific Management Review 27:50–57. https://doi.org/10.1016/j.apmrv.2021.05.002
8. Gibson D, EY (2020) How to protect your workforce, operations and values during COVID-19. International Tax Review N.PAG
9. Ratten V, Thaichon P (2021) COVID-19, Technology and Marketing Moving Forward and the New Normal
10. Meironke A, Kuehnel S (2022) Association for Information Systems Association for Information Systems AIS Electronic Library (AISeL) AIS Electronic Library (AISeL) How to Measure RPA's Benefits? A Review on Metrics, Indicators, How to Measure RPA's Benefits? A Review on Metrics, Indic
11. Martins CMG, Mamede H, da Silva MLBM (2018) Robotic Process Automation A Lean Approach to RPA Information Systems and Computer Engineering Examination Committee
12. Kosi F (2019) Robotic Process Automation (RPA) and Security. 1–36
13. Santos F, Pereira R, Vasconcelos JB (2020) Toward robotic process automation implementation: an end-to-end perspective. Business Process Management Journal 26:405–420. https://doi.org/10.1108/BPMJ-12-2018-0380
14. ISO/PAS 22399:2007 - Societal security - Guideline for incident preparedness and operational continuity management. https://www.iso.org/standard/50295.html. Accessed 2 Apr 2023
15. (2003) ISO/IEC 15504-2:2003 - Information technology — Process assessment — Part 2: Performing an assessment. https://www.iso.org/standard/37458.html. Accessed 7 Apr 2023
16. Moving from BS 25999-2 to ISO 22301. https://www.bsigroup.com/documents/iso-22301/resources/bsi-bs25999-to-iso22301-transition-uk-en.pdf. Accessed 4 Apr 2023
17. (2015) ISO/IEC 33020:2015 - Information technology — Process assessment — Process measurement framework for assessment of process capability. https://www.iso.org/standard/54195.html. Accessed 7 Apr 2023
18. (2010) ISO/IEC TR 18018:2010 - Information technology — Systems and software engineering — Guide for configuration management tool capabilities. https://www.iso.org/standard/51042.html. Accessed 7 Apr 2023

19. ISO/IEC 27031:2011(en), Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en. Accessed 21 Aug 2022
20. BS25999, BS 25999. https://web.archive.org/web/20061015195123/http://www.pas56.com/support.htm. Accessed 4 Apr 2023
21. BS 25999 and its Contribution to Business Continuity Management | BSI Middle East and Africa. https://www.bsigroup.com/en-AE/About-BSI/Media-Center/Press-releases/2011/6/BS-25999-and-its-Contribution-to-Business-Continuity-Management/. Accessed 4 Apr 2023
22. SI 24001: Organizational resilience management system (ORMS) – Requirements and guidance for use - Standards Institution of Israel. https://www.sii.org.il/en/24001. Accessed 2 Apr 2023
23. ASIS International and BSI release joint business continuity management ANSI standard. https://www.continuitycentral.com/news05526.html. Accessed 2 Apr 2023
24. PAS56, PAS 56 and BS25999 Business Continuity Management. https://web.archive.org/web/20061015195120/http://www.pas56.com/. Accessed 23 Feb 2023
25. Cascais Brás J, Pereira RF, Moro S, et al (2023) Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019. IEEE Access 11:134239–134258. https://doi.org/10.1109/ACCESS.2023.3337159
26. (2012) ISO 22301:2012(en), Societal security — Business continuity management systems --- Requirements
27. ISO/TS 22332:2021 - Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures. https://www.iso.org/standard/50069.html. Accessed 4 Nov 2023
28. Brás J, Pereira R, Moro S (2023) Intelligent Process Automation and Business Continuity: Areas for Future Research. Information 2023, Vol 14, Page 122 14:122. https://doi.org/10.3390/INFO14020122
29. Siderska J (2021) The Adoption of Robotic Process Automation Technology to Ensure Business Processes during the COVID-19 Pandemic. Sustainability 2021, Vol 13, Page 8020 13:8020. https://doi.org/10.3390/SU13148020
30. José Cascais Brás;, Ribeiro R (2016) Business Continuity and Disaster Recovery: New Trends and Challenges. 13th CONTECSI - International Conference on Information Systems and Technology Management. https://doi.org/10.5748/9788599693124-13CONTECSI/RF-3893
31. ISO 22313:2020(en) Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
32. Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive) | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive. Accessed 10 Dec 2023
33. Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554. https://www.digital-operational-resilience-act.com/. Accessed 10 Dec 2023
34. IEEE (2017) IEEE Guide for Terms and Concepts in Intelligent Process Automation. IEEE_Std_2755-2017 1–16. https://doi.org/DOI: 10.1109/IEEESTD.2017.8070671
35. Kregel I, Koch J, Plattfaut R (2021) Beyond_the_Hype:Robotic_Process_Automation's_Public_Perception_Over_Time. Journal_of_Organizational_Computing_and_Electronic_Commerce 31:130–150. https://doi.org/10.1080/10919392.2021.1911586
36. IEEE SA Bringing Clarity and Objective Guidance to Software Based Intelligent Process Automation Space. https://beyondstandards.ieee.org/ieee-2755-standards-to-bring-clarity-and-objective-guidance-to-software-based-intelligent-process-automation-space/. Accessed 22 Mar 2023
37. Ivančić L, Vugec D, … VV-C on BP, 2019 U (2019) Robotic process automation: systematic literature review. Springer
38. Garousi V, Felderer M, Mäntylä M V. (2019) Guidelines_for_including_grey_literature_and_conducting_multivocal_literature_reviews_in_software_engineering. Information_and_Software_Technology 106:101–121. https://doi.org/10.1016/j.infsof.2018.09.006
39. Garousi V, Felderer M, Mäntylä M V. (2016) The_need_for_multivocal_literature_reviews_in_software_engineering. 1–6. https://doi.org/10.1145/2915970.2916008
40. Kitchenham B (2007) Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering
41. Van den Oever B (2020) Method for estimating the impact of Robotic Process Automation implementations on business processes.
42. Amaro R, Pereira R, Mira M DevOps Capabilities and Practices : A Multivocal Literature Review. 1–19

43. Pokhrel A, Katta V, Colomo-Palacios R (2020) Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review. Proceedings - 2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops, ICSEW 2020 671–678. https://doi.org/10.1145/3387940.3392199
44. Ogawa RT, Malen B (1991) Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method. Rev Educ Res 61:265–286. https://doi.org/10.3102/00346543061003265
45. Garousi V, Felderer M, Mäntylä M V. (2019) Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf Softw Technol 106:101–121. https://doi.org/10.1016/j.infsof.2018.09.006
46. Garousi V, Felderer M, Mäntylä M V. (2016) The need for multivocal literature reviews in software engineering. 1–6. https://doi.org/10.1145/2915970.2916008
47. Swain AK, Garza VR (2023) Key Factors in Achieving Service Level Agreements (SLA) for Information Technology (IT) Incident Resolution. Information Systems Frontiers 25:819–834. https://doi.org/10.1007/S10796-022-10266-5/FIGURES/1
48. Google Robotic Process Automation - Explorar - Google Trends. https://trends.google.com/trends/explore?date=all&q=Robotic%20Process%20Automation&hl=pt-PT. Accessed 3 Nov 2023
49. Chugh R, Macht S, Hossain R (2022) Robotic_Process_Automation:a_review_of_organizational_grey_literature. International_Journal_of_Information_Systems_and_Project_Management 10:5–26. https://doi.org/10.12821/ijispm100101
50. Aldossari M, Zin AM (2019) The_use_of_automation_and_robotic_innovations_in_the_transformational_companies:Systematic_literature_review. Journal_of_Theoretical_and Applied_Information_Technology 97:3661–3690
51. Theuerkauf J (2021) Rethinking Business Continuity Plans, Phase One: Initializing RPA Deployment. https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/06/19/rethinking-business-continuity-plans-phase-one-initializing-rpa-deployment/?sh=42b038514bdc. Accessed 25 Jul 2023
52. PwC (2016) Robotic Process Automation – friend or foe for your risk profile? https://www.pwc.com.au/pdf/pwc-article-rpa-friend-or-foe-for-your-risk-profile.pdf. Accessed 5 Nov 2023
53. Păunescu C, Argatu R (2020) Critical_functions_in_ensuring_effective_business_continuity_management.Evidence_from_Romanian_companies. Journal_of_Business-Economics_and_Management 21:497–520. https://doi.org/10.3846/JBEM.2020.12205
54. Mccolum T (2018) The Risk of a Narcissistic CEO. Internal Auditor
55. Stansfield C, Dickson K, Bangpan M (2016) Exploring_issues_in_the_conduct_of_website_searching_and_other_online_sources_for_systematic_reviews:How_can_we_be_systematic? Systematic_Reviews 5:1–9. https://doi.org/10.1186/s13643-016-0371-9
56. Bellefontaine SP, Lee CM (2014) Between Black and White: Examining Grey Literature in Meta-analyses of Psychological Research. J Child Fam Stud 23:1378–1388. https://doi.org/10.1007/s10826-013-9795-1
57. Coleman S, Wright JM, Nixon J, et al (2020) Searching_for_Programme_theories_for_a_realist_evaluation:A_case_study_comparing_an_academic_database_search_and_a_simple_ Google_search. BMC_Medical_Research_Methodology 20:1–10. https://doi.org/10.1186/s12874-020-01084-x
58. Wohlin C (2014) Guidelines for snowballing in systematic literature studies and a replication in software engineering. ACM International Conference Proceeding Series. https://doi.org/10.1145/2601248.2601268
59. Garousi V, Felderer M, Mäntylä M V. (2019) Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf Softw Technol 106:101–121. https://doi.org/10.1016/J.INFSOF.2018.09.006
60. Lacity M, Willcocks L (2017) Robotic Process Automation and Risk Mitigation: The Definitive Guide. SB Publishing
61. Jain N (2020) The risk of RPA implementation and how to mitigate it. https://www.capgemini.com/2020/09/the-risk-of-rpa-implementation-and-how-to-mitigate-it/. Accessed 20 Mar 2023
62. Liao X (2019) Top 8 risks associated with RPA and how to mitigate them
63. Kedziora D (2021) Robotic Process Automation (RPA) Implementation Drivers: Evidence of Selected Nordic Companies. Issues in Information Systems 22:21–40. https://doi.org/10.48009/2_iis_2021_21-40
64. Todorov R (2018) Approaching Robotic Process Automation with confidence Robotic Process Automation - In a nutshell. 14

65. Tucci L (2021) Ultimate Guide to RPA (Robotic Process Automation). https://searchcio.techtarget.com/Ultimate-guide-to-RPA-robotic-process-automation. Accessed 11 Jan 2023
66. Schatz J (2019) Considering RPA? Make sure you understand the security implications -- GCN. https://gcn.com/articles/2019/12/18/rpa-security.aspx. Accessed 5 Oct 2023
67. Loon van B, Juttmann J, Chuah H, Pouwer M (2018) Adding value through governance, risk management, and controls. KPMG
68. Kedziora D, Penttinen E (2020) Governance models for robotic process automation: The case of Nordea Bank: https://doi.org/101177/2043886920937022 11:20–29. https://doi.org/10.1177/2043886920937022
69. Deloitte (2018) Internal Controls Over Financial Reporting Considerations for Developing and Implementing Bots. 1–8
70. Arun T (2020) Robotic Process Automation (RPA): Risks and Controls | by Arun Thomas | Medium. https://medium.com/@netsentries/robotic-process-automation-rpa-risks-and-controls-9afb96f7fcb3. Accessed 26 Apr 2023
71. Dilmegani C (2017) What is Robotic Process Automation (RPA)? Ultimate Guide. https://research.aimultiple.com/rpa/. Accessed 14 Jun 2023
72. Kirchmer M (2017) Robotic Process Automation – Pragmatic Solution or Dangerous Illusion? https://insights.btoes.com/risks-robotic-process-automation-pragmatic-solution-or-dangerous-illusion. Accessed 15 Jun 2023
73. Crane D Contractual considerations in Robotic Process Automation and Artificial Intelligence outsourcing | McCarthy Tétrault. In: 2018. https://www.mccarthy.ca/en/insights/blogs/snipits/contractual-considerations-robotic-process-automation-and-artificial-intelligence-outsourcing. Accessed 11 Jan 2023
74. Gilmurray K (2021) 14 rules for Robotic Process Automation (RPA) and Intelligent Automation (AI) success - The AI Journal. https://aijourn.com/14-rules-for-robotic-process-automation-rpa-and-intelligent-automation-ai-success/. Accessed 8 May 2023
75. Berg R (2018) Five Robotic Process Automation (RPA) Myths. https://content.quanton.co.nz/blog/five-robotic-process-automation-rpa-myths. Accessed 10 May 2023
76. Lowes P, Cannata FRS, Chitre S, Barkham J (2017) Automate this: The business leader's guide to robotic process automation. Deloitte Development LLC 1–25
77. Holmlund P (2020) The pros and cons of RPA: Is it the best choice for your business? | Qvalia. https://qvalia.com/blog/the-pros-and-cons-of-rpa-is-it-the-best-choice-for-your-business/. Accessed 15 Jun 2023
78. Gotthardt M, Koivulaakso D, Paksoy O, et al (2020) ACRN Journal of Finance and Risk Perspectives Current State and Challenges in the Implementation of Smart Robotic Process Automation in Accounting and Auditing. ACRN Journal of Finance and Risk Perspectives 9:90–102. https://doi.org/10.35944/jofrp.2020.9.1.007
79. Mitra S (2019) Robotic Process Automation Adoption Challenges & Solutions | EPAM. https://www.epam.com/about/newsroom/in-the-news/2019/rpas-adoption-challenges-and-how-to-solve-them. Accessed 8 Jun 2023
80. Models B (2017) Understanding robotic process automation (RPA). the Capco Institute Journal of Financial Transformation 46:
81. blueprint (2021) 7 Hidden Risks of Automation Design in Business | Blueprint. https://www.blueprintsys.com/blog/rpa/7-hidden-risks-automation-design. Accessed 11 Jun 2023
82. J. Juttmann, M. van Doesburg (2018) Robotic Process Automation: how to move on from the proof of concept phase? - Compact. https://www.compact.nl/articles/robotic-process-automation-how-to-move-on-from-the-proof-of-concept-phase/. Accessed 27 May 2023
83. Kirchmer M, Franz P (2019) Value-Driven Robotic Process Automation (RPA): A Process-Led Approach to Fast Results at Minimal Risk. Lecture Notes in Business Information Processing 356:31–46. https://doi.org/10.1007/978-3-030-24854-3_3
84. Hawkins I (2019) A Guide to Robotic Process Automation (RPA) - iGrafx. https://www.igrafx.com/a-guide-to-robotic-process-automation-rpa/. Accessed 17 Jun 2023
85. Hugo Ciopages (2016) Robotic Process Automation: The opportunity, risks and rewards. https://www.ciopages.com/robotic-process-automation/. Accessed 4 Jun 2023
86. i-SCOOP (2020) Robotic Process Automation (RPA): definition, benefits and usage. https://www.i-scoop.eu/robotic-process-automation-rpa/. Accessed 4 May 2023
87. Jędrzejka D (2019) Robotic process automation and its impact on accounting. Zeszyty Teoretyczne Rachunkowości 2019:137–166. https://doi.org/10.5604/01.3001.0013.6061

88. Bradford S, Landrum K (2019) Robotic Process Automation: 4 Key Considerations. https://www.informationweek.com/ai-or-machine-learning/robotic-process-automation-4-key-considerations. Accessed 11 Jun 2023
89. BBI (2018) What is Robotic Process Automation – Benefits and Real-life Cases - Data Driven Digital Transformation | BBI. https://bbi-consultancy.com/robotic-process-automation-benefits/. Accessed 5 Jun 2023
90. Pluzhnikov O (2020) Top 10 security risks of RPA. eleks
91. Szalony S, Salkin P, Sewell K (2019) The 3 Rs of Finance Automation: RPA, Risk, Rewards - WSJ. https://deloitte.wsj.com/articles/the-3-rs-of-finance-automation-rpa-risk-rewards-01574283372. Accessed 27 May 2023
92. Willcocks L, Craig A (2020) Business automation in investment banking: fast forward…. or not? | LSE Business Review. https://blogs.lse.ac.uk/businessreview/2020/01/27/business-automation-in-investment-banking-fast-forward-or-not/. Accessed 17 Jun 2023
93. Beroe Inc (2021) Robotic Process Automation Prone to Cyber Attacks. https://www.beroeinc.com/blog/robotic-process-automation-prone-to-cyber-attacks/. Accessed 15 May 2023
94. Violino B (2020) 6 hidden risks of IT automation. https://www.cio.com/article/190962/6-hidden-risks-of-it-automation.html. Accessed 9 Jan 2023
95. Moffitt KC, Rozario AM, Vasarhelyi MA (2018) Robotic Process Automation for Auditing. Journal of Emerging Technologies in Accounting 15:1–10. https://doi.org/10.2308/JETA-10589
96. Gampe P (2021) Hyper-automation: Hype or help for businesses? | ITProPortal. https://www.itproportal.com/features/hyper-automation-hype-or-help-for-businesses/. Accessed 15 May 2023
97. Spencer J (2020) Beware The Hidden Dangers Of Robotic Process Automation. https://iig.technology/beware-the-hidden-dangers-of-robotic-process-automation/. Accessed 13 Jun 2023
98. Smith P (2019) All you need to know about implementing robotic process automation | ACCA Global. https://www.accaglobal.com/ca/en/member/discover/cpd-articles/business-management/rpajun19-cpd.html. Accessed 15 Jun 2023
99. ProV (2021) Robot Failure: Best Practices for Robotics Process Automation Development
100. Zaharia-Radulescu A-M, Pricop CL, Shuleski D, Ioan AC (2017) RPA and the future of workforce. Proceedings of the international management conference 11:384–392
101. Casey K (2020) Robotic Process Automation (RPA): What you need to know about security | The Enterprisers Project. https://enterprisersproject.com/article/2020/7/rpa-robotic-process-automation-security. Accessed 26 Apr 2023
102. Joshi N (2019) Leverage RPA, But Plan For Its Inherent Risks, Too! https://www.forbes.com/sites/cognitiveworld/2019/06/28/leverage-rpa-but-plan-for-its-inherent-risks-too/?sh=58aebc2a11d1. Accessed 9 Jan 2023
103. Bednarz M (2020) 7 Keys to Successful Robotics Process Automation - New Jersey Business Magazine. https://njbmagazine.com/njb-news-now/7-keys-to-proper-robotics-process-automation/. Accessed 5 Jun 2023
104. Murphy KL Robotic Process Automation and Low-Code. In: 2018. https://www.outsystems.com/blog/posts/robotic-process-automation-low-code/. Accessed 11 Jan 2023
105. Pritchard S (2021) How robotic process automation is getting smarter as it evolves. https://www.computerweekly.com/feature/How-robotic-process-automation-is-getting-smarter-as-it-evolves. Accessed 28 Apr 2023
106. van der Aalst WMP, Bichler M, Heinzl A (2018) Robotic Process Automation. Business and Information Systems Engineering 60:269–272. https://doi.org/10.1007/S12599-018-0542-4
107. Automation Anywhere (2021) What is RPA? Robotic Process Automation | Automation Anywhere. https://www.automationanywhere.com/rpa/robotic-process-automation. Accessed 8 May 2023
108. AUDITBOARD (2018) What Is Robotic Process Automation? Can It Assist Internal Audit? | AuditBoard. https://www.auditboard.com/blog/5-ways-robotics-process-automation-can-assist-internal-audit/. Accessed 19 Jun 2023
109. West DM (2021) How robotic process and intelligent automation are altering government performance. https://www.brookings.edu/research/how-robotic-process-and-intelligent-automation-are-altering-government-performance/. Accessed 26 Apr 2023
110. ISACA (2020) The Dark Side of Robotic Process Automation. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/the-dark-side-of-robotic-process-automation. Accessed 24 Oct 2023
111. Alvarez C, Salazar N (2020) Robotic Process Automation Risk and Chanllenges - Summer 2020 Prof. Vasarhelyi - YouTube. YouTube

112. SolveXia (2019) Everything you Need to Know about Robotic Process Automation. https://www.solvexia.com/blog/everything-to-know-robotic-process-automation. Accessed 11 Jun 2023
113. Kelly M (2019) What Is Robotic Process Automation & Why Should Compliance Care About It? | Risk & Compliance Matters by NAVEX. https://www.navexglobal.com/blog/article/what-is-robotic-process-automation-why-should-compliance-care-about-it/. Accessed 13 Jun 2023
114. Martin R, Flaherty J, Hansen K (2019) How automation is evolving the role of Internal Audit in Healthcare Robotics Process Automation : How automation is evolving the role of Internal Audit in Healthcare
115. Frankenfield J (2017) Robotic Process Automation (RPA) Definition. https://www.investopedia.com/terms/r/robotic-process-automation-rpa.asp. Accessed 4 Jun 2023
116. Gomez G (2020) What is Intelligent Process Automation (IPA)? https://www.bizagi.com/en/blog/intelligent-process-automation/what-is-intelligent-process-automation-ipa. Accessed 14 Jun 2023
117. Wyn S, Canterbury J (2020) A GAMP® Approach to Robotic Process Automation | Pharmaceutical Engineering. https://ispe.org/pharmaceutical-engineering/gamp-approach-robotic-process-automation. Accessed 14 Jun 2023
118. CiGen (2020) 3 Ways to Settle RPA and Intelligent Automation Fears in Your Organisation – CiGen. https://www.cigen.com.au/3-ways-settle-rpa-intelligent-automation-fears/. Accessed 16 Jun 2023
119. PwC (2018) Robotic process automation : A primer for internal audit professionals. Pwc 1–4
120. Kaur J (2021) Understanding Robotic Process Automation in Cybersecurity. https://www.xenonstack.com/insights/rpa-security-risk-management. Accessed 8 May 2023
121. Lawton G (2021) What Is Robotic Process Automation (RPA)? Everything You Need to Know. https://www.techtarget.com/searchcio/definition/RPA. Accessed 12 Apr 2023
122. Balicki A (2017) Can Robotic Process Automation reduce Operational Risk to zero? | LinkedIn. https://www.linkedin.com/pulse/can-robotic-process-automation-reduce-operational-risk-artur-balicki/. Accessed 27 May 2023
123. Matteson S (2021) How Robotic Process Automation can make work more efficient in your business - TechRepublic. https://www.techrepublic.com/article/how-robotic-process-automation-can-make-work-more-efficient-in-your-business/. Accessed 8 Oct 2023
124. Kuppinger M (2019) Robotic Process Automation – an IAM Challenge | KuppingerCole. https://www.kuppingercole.com/blog/kuppinger/robotic-process-automation-an-iam-challenge. Accessed 11 Jun 2023
125. Bubniuk N (2020) Turbo-Charging Business Operations with Robotic Process Automation - Intellias. https://intellias.com/robotic-process-automation-use-cases/. Accessed 11 Jun 2023
126. Limited I (2020) View Point Security Considerations in Robotic Process Automation
127. Hutchins C (2021) Robotic Process Automation (RPA): Use Cases And Risks To Consider. https://www.cioapplications.com/cxoinsights/robotic-process-automation-rpa-use-cases-and-risks-to-consider-nid-4073.html. Accessed 17 Jun 2023
128. Goswami S (2019) Robotic Process Automation: Security Essentials. https://www.bankinfosecurity.com/interviews/robotic-process-automation-security-issues-i-4480. Accessed 11 Jun 2023
129. Murugappan K, Sree Kala T, Forensics TSK-CS and D, 2022 U (2021) An Enhanced Security Framework for Robotic Process Automation. Springer 231–238. https://doi.org/10.1007/978-981-16-3961-6_20
130. Babic S (2021) Tips for robotic process automation success: Part 2 - The Hyland Blog. https://blog.hyland.com/robotic-process-automation/tips-for-robotic-process-automation-success-part-2/. Accessed 4 May 2023
131. Tornbohm C (2021) #HowTo: Stay Secure When Deploying Robotic Process Automation - Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/secure-robotic-process-automation/. Accessed 4 Jun 2023
132. Jeffs A, Hawkins I (2021) PEX Guide: What is robotic process automation (RPA)? | Process Excellence Network. https://www.processexcellencenetwork.com/rpa-artificial-intelligence/articles/a-guide-to-robotic-process-automation-rpa. Accessed 26 Apr 2023
133. Reciprocity (2021) Compliance Considerations for Robotic Process Automation — Reciprocity. https://reciprocity.com/compliance-considerations-for-robotic-process-automation/. Accessed 4 May 2023
134. Wiggers K (2021) A definitive primer on robotic process automation | VentureBeat. https://venturebeat.com/2021/05/02/what-is-robotic-process-automation/. Accessed 3 Apr 2023
135. CIOReview (2019) Risk and Control Considerations within an RPA Platform. https://www.cioreview.com/news/risk-and-control-considerations-within-an-rpa-platform--nid-29055-cid-75.html. Accessed 11 Jun 2023

136. Séguin S, Tremblay H, Benkalaï I, et al (2021) Minimizing the number of robots required for a Robotic Process Automation (RPA) problem. Procedia Comput Sci 192:2689–2698. https://doi.org/10.1016/j.procs.2021.09.039
137. Eikebrokk TR, Olsen DH (2020) Robotic Process Automation and Consequences for Knowledge Workers; a Mixed-Method Study. Responsible Design, Implementation and Use of Information and Communication Technology 12066:114. https://doi.org/10.1007/978-3-030-44999-5_10
138. Wright D, Witherick D, Gordeeva M (2018) The robots are ready. Are you? Untapped advantage in your digital workforce. Deloitte Development LLC 24
139. Richardson S (2020) Cognitive automation: A new era of knowledge work? Business Information Review 37:182–189. https://doi.org/10.1177/0266382120974601
140. Werner M (2014) BUSINESS PROCESS ANALYSIS AUTOMATION FOR FINANCIAL AUDITS A design science-oriented approach to support internal and external auditors in pro-cess audits by using process mining techniques Kumulative Dissertation
141. Hanna S (2021) Too many tasks, too little time: Robotic process automation can help | Healthcare IT News. https://www.healthcareitnews.com/blog/too-many-tasks-too-little-time-robotic-process-automation-can-help. Accessed 10 May 2023
142. Ågnes JS (2022) Gaining and Training a Digital Colleague: Employee Responses to Robotization. Journal of Applied Behavioral Science 58:29–64. https://doi.org/10.1177/00218863211043596
143. Dunn M (2021) See why robotic process automation for due diligence has gained momentum and the advantages companies can realize from it. | BIS UK Blog. https://bis.lexisnexis.co.uk/blog/categories/governance-risk-and-compliance/automating-due-diligence-RPA. Accessed 8 Jun 2023
144. Raiker RM (2018) Intelligent Process Mining in Robotic Process Automation | by Ryan M. Raiker, MBA | Towards Data Science. https://towardsdatascience.com/intelligent-process-mining-in-robotic-process-automation-f684dd4c7de5. Accessed 17 Jun 2023
145. Enriquez JG, Jimenez-Ramirez A, Dominguez-Mayo FJ, Garcia-Garcia JA (2020) Robotic Process Automation: A Scientific and Industrial Systematic Mapping Study. IEEE Access 8:39113–39129. https://doi.org/10.1109/ACCESS.2020.2974934
146. Hunsaker M, Papenfuss D (2020) Fraud and Emerging Tech: Robotic Process Automation - FEI. https://www.financialexecutives.org/FEI-Daily/January-2020/Fraud-and-Emerging-Tech-Robotic-Process-Automatio.aspx. Accessed 11 Jun 2023
147. Rashid N (2021) 4 Steps To Ensure Robotic Process Automation Security | CDOTrends. https://www.cdotrends.com/story/15504/4-steps-ensure-robotic-process-automation-security. Accessed 15 May 2023
148. Sakpal M (2021) How to Ensure Robotic Process Automation Security. https://www.gartner.com/smarterwithgartner/4-steps-to-ensure-robotic-process-automation-security. Accessed 9 Jan 2023
149. Minolta K (2020) Robotic process automation: when everything runs automatically | KONICA MINOLTA. https://www.konicaminolta.eu/eu-en/rethink-work/tools/rpa-what-exactly-is-robotic-process-automation. Accessed 5 Jun 2023
150. Chacón-Montero J, Jiménez-Ramírez A, Enríquez JG (2019) Towards a method for automated testing in robotic process automation projects. Proceedings - 2019 IEEE/ACM 14th International Workshop on Automation of Software Test, AST 2019 42–47. https://doi.org/10.1109/AST.2019.00012
151. Pokhrel A, Katta V, Colomo-Palacios R (2020) Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review. Proceedings - 2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops, ICSEW 2020 671–678. https://doi.org/10.1145/3387940.3392199
152. Russo N, Mamede HS, Reis L, et al (2023) Exploring a Multidisciplinary Assessment of Organisational Maturity in Business Continuity: A Perspective and Future Research Outlook. Applied Sciences 2023, Vol 13, Page 11846 13:11846. https://doi.org/10.3390/APP132111846

Chapter 6

Article nr. #5 – “Balancing Business, IT, and Human Capital: RPA Integration and Governance Dynamics.”

This article provides significant insights into the dynamics of integrating RPA with governance, business, and IT, emphasizing its profound impact on human capital. Through a comprehensive multivocal literature review, the article offers crucial insights into the challenges and best practices of integrating RPA into corporate governance structures.

The study explores the intricate relationship between business, IT, and RPA governance, detailing how process automation can be effectively managed to foster procedural standardization, enhance efficiency, and ensure compliance with regulatory frameworks. It further underlines the vital role of change management and employee engagement in securing the successful implementation of RPA initiatives, highlighting the importance of upskilling and empowering employees to work effectively alongside automated systems.

The article also emphasizes that human capital management is essential in the age of automation. It calls attention to the need for organizations to cultivate a culture of continuous learning and adaptability, preparing employees to embrace automation technologies. This research sheds light on the complexities involved in aligning RPA integration with governance frameworks, stressing that automation technologies must contribute to organizational efficiency without compromising compliance or operational integrity.

Article Details:

- Title: "Balancing Business, IT, and Human Capital: RPA Integration and Governance Dynamics."
- Submission Date: 03/05/2023
- Journal: Sage Open
- Publisher: SAGE Publishing
- Submission Date: 03/05/2023
- Scimago Journal Rank: Quartile 1 – Business and Management

Sage Open

Balancing Business, IT, and Human Capital: RPA Integration and Governance Dynamics

Journal:	*Sage Open*
Manuscript ID	SO-24-1307
Manuscript Type:	Literature Review
Main Discipline or Subject Area:	Business & Management
Keywords:	Robotic Process Automation, Governance, Risk, Data Processing and Interpretation < Research Methods < Social Sciences, Corporate Governance < Business Law and Business Ethics < Management < Social Sciences, Risk Communication < Human Communication < Communication Studies < Communication < Social Sciences
Approaches:	Mixed
Methods:	Systematic Literature Review

Abstract:	In the era of technological progress, Robotic Process Automation has emerged as a pivotal tool in professional domains. Companies are diligently pursuing process automation to reinforce operational efficiency, amplify productivity, control costs, and minimize procedural errors. Robotic Process Automation, a specialized software, is tailored for the mechanization of repetitive tasks, previously laboriously undertaken by human resources. Its effectiveness centers on seamless integration within business, information technology, and human resource realms. To provide a comprehensive understanding, an extensive multivocal literature review encompassing eighty-six documents, spanning conventional and non-traditional sources, was conducted. This review encompassed topics including Robotic Process Automation, governance, auditing, and policies. Additionally, interviews were conducted to glean firsthand insights, experiences, and diverse perspectives on the subject. This study's primary contributions lie in elucidating the nexus between business processes and information technology, fostering procedural standardization, ensuring compliance with regulatory frameworks, engendering employee engagement, delineating shifts in roles and responsibilities, and prudently managing organizational change. These insights significantly enhance the likelihood of successful Robotic Process Automation initiatives while prudently mitigating associated risks.

SO-24-1307

Plain Language Summary Title:

â€˜N/Aâ€™ if not applicable

Plain Language Summary:

â€˜N/Aâ€™ if not applicable

Balancing Business, IT, and Human Capital: RPA Integration and Governance Dynamics

José Cascais Brás [a *], Ruben Filipe Pereira [a], Marcella Melo[a]

Sérgio Moro [a], *Isaias Scalabrin Bianchi* [b]

(a) Instituto Universitário de Lisboa (ISCTE-IUL), Portugal;
(B) Federal University of Sana Catarina, Brazil.
(*) Corresponding Author: jose_manuel_bras@iscte-iul.pt;

Marcella Melo:

https://orcid.org/0009-0009-5419-9645

Abstract: In the era of technological progress, Robotic Process Automation has emerged as a pivotal tool in professional domains. Companies are diligently pursuing process automation to reinforce operational efficiency, amplify productivity, control costs, and minimize procedural errors. Robotic Process Automation, a specialized software, is tailored for the mechanization of repetitive tasks, previously laboriously undertaken by human resources. Its effectiveness centers on seamless integration within business, information technology, and human resource realms. To provide a comprehensive understanding, an extensive multivocal literature review encompassing eighty-six documents, spanning conventional and non-traditional sources, was conducted. This review encompassed topics including Robotic Process Automation, governance, auditing, and policies. Additionally, interviews were conducted to glean firsthand insights, experiences, and diverse perspectives on the subject. This study's primary contributions lie in elucidating the nexus between business processes and information technology, fostering procedural standardization, ensuring compliance with regulatory frameworks, engendering employee engagement, delineating shifts in roles and responsibilities, and prudently managing organizational change. These insights significantly enhance the likelihood of successful Robotic Process Automation initiatives while prudently mitigating associated risks.

Keywords: Robotic Process Automation, Governance, Risk, Compliance

1. Introduction

The nomenclature "Robotic Process Automation" (RPA) surfaced in the early 2000s, denoting a methodology for the automation of processes or tasks employing robotic entities. These agents supplant human intervention in scenarios characterized by repetitiveness and clearly delineated parameters, or alternatively, they cooperate with human agents in a blended mode of operation [1]. As depicted in Figure 1, the graphical representation illustrates the escalating trajectory of global Google search inquiries for "Robotic Process Automation" within the temporal span from 2012 to 2023.

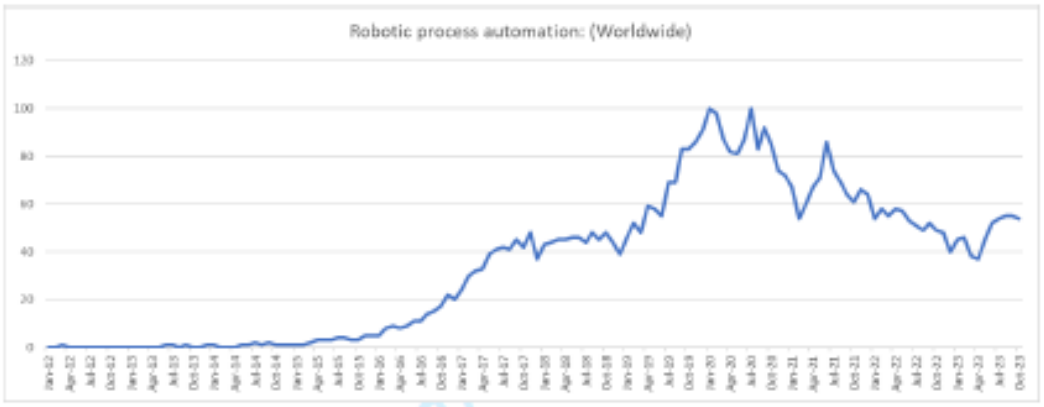


Figure 6.1 - Google Trend for Robotic Process Automation

RPA encompasses a spectrum of applications, yielding heightened operational efficiency, amplified productivity, and cost mitigation. Tasks encompassing data entry into forms [2], data aggregation within tables [3], rule-based processes or tasks [4], and iterative interactions [4] with applications stand as exemplars of actions amenable to RPA execution. Noteworthy is American Express Global Business Travel's utilization of RPA, particularly in the domain of airline ticket cancellations, with an envisioned expansion towards automating airport tasks and proffering recommendations to clientele [5]. It is crucial to underscore that RPA's deployment is not tantamount to wholesale employee displacement, but rather an instrumental means to alleviate personnel from non-value-added pursuits, thereby affording them the capacity to concentrate on tasks necessitating human intervention or overseeing the outcomes of automated endeavors [6].

Presently, companies embarking on a trajectory with RPA evince a more circumspect outlook regarding anticipated returns, in stark contrast to the initial surge in popularity of this technology. The realization of optimal value hinges upon managerial oversight to ensure the concurrent implementation and maintenance of multiple robotic entities, thus engendering inquiries pertaining to governance and its judicious application [1], [7]. Empirical evidence gleaned from a survey encompassing 250 enterprises delineates that 12% have operationalized RPA, with half of these entities attaining a favorable Return on Investment (ROI) within an 18-month timeframe [8].

Several factors may impede the attainment of prescribed corporate objectives. It is imperative to fathom how a paucity of collaborative endeavors exerts influence [3], [7], [9], in addition to the nexus with compliance [3], [10]– [12], and sundry other pertinent

considerations. This study is motivated by the aspiration to scrutinize and interrelate the governance frameworks governing RPAs with the spheres of Business, Information Technology (IT), and Human Resources, while concurrently elucidating their interface with audit practices and organizational policies.

Hence, this article aims to focus on one main research question:

> RQ1 - What is the impact of RPA governance on the dynamic interrelationships among Business, IT, and People, in conjunction with audit practices and organizational policies within organisations?

2. Background

2.1. Robotic Process Automation

Currently, within the existing body of literature, diverse definitions of RPA are discernible. Several scholarly contributions characterize RPA as a framework designed to automate repetitive tasks within business processes, employing software agents proficient in emulating human interactions with graphical interfaces [13]–[15].

It is important to emphasize that RPA is a software-based system, devoid of physical instantiation, and capable of interfacing with various applications or digital systems for tasks encompassing data input, extraction, and manipulation. This functionality is executed through software entities commonly referred to as bots. An illustrative case study from Infosys reveals a 58% reduction in manual labor following RPA implementation, signifying not a diminution in personnel but an amplification of their productivity through the adept use of bots as agile assistants [9].

In contrast to traditional coding paradigms, RPA development operates on pre-defined code components, enabling developers to incorporate and configure activities through an intuitive interface [16]. This streamlined development process translates into brief training intervals for staff, equipping them with the requisite proficiency in configuration and deployment. While the implementation process is characterized by relative straightforwardness, it is advised against excluding IT departments from the decision-making process, given their overarching responsibility for governance, infrastructure, and security [5], [7]. Moreover, RPA is particularly efficacious in contexts characterized by process standardization, rule-based frameworks, and discernible levels of interaction and complexity [6].

Notwithstanding its capacity for facilitating expeditious and uncomplicated automation, the establishment of robust governance frameworks for RPA initiatives poses a substantive challenge. When an organization chooses to assimilate RPA comprehensively into its operational architecture, as opposed to deploying it as a discrete solution, the ensuing proliferation of bots engenders heightened complexity in governance requirements [18].

2.2. Governance

Governance can be elucidated as a multifaceted process encompassing decision-making, alongside the subsequent execution or abstention from implementing choices by individuals occupying positions of authority. This concept finds application across diverse domains, including the sphere of corporate governance [19].

Distinct forms of governance emerge contingent upon the specific domain under consideration. For instance, as depicted in Figure 2, corporate governance primarily pertains to the operational milieu of businesses. Conversely, IT governance is germane to the realm of information technology. Additionally, there exist other classifications not explicitly delineated in the figure, such as environmental governance, which centers on matters pertaining to environmental management and related concerns [20].

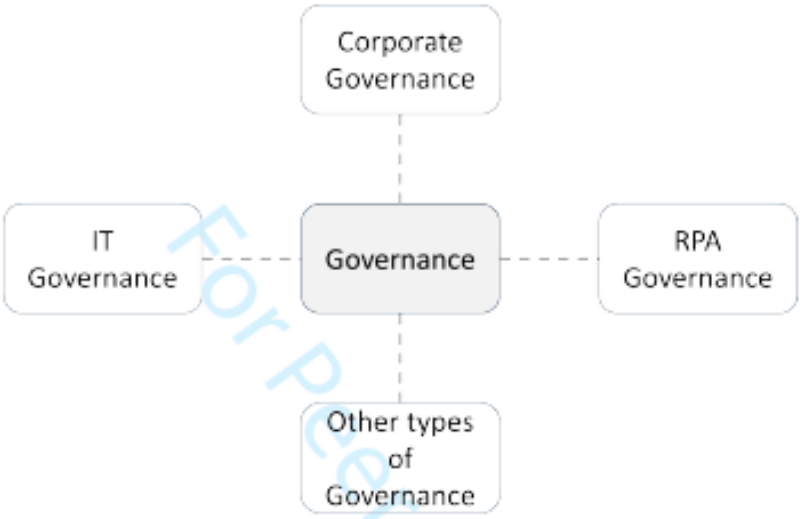


Figure 6.2 - Types of governance.

Corporate governance

Corporate governance pertains to a comprehensive framework comprising practices, statutory provisions, procedural protocols, and guiding principles intended to enhance overall business administration. Its fundamental objective lies in harmonizing the interests of diverse stakeholders, including shareholders, employees, and suppliers, among others [21]. Inadequate adherence to robust corporate governance standards can precipitate challenges in goal attainment, produce diminished support from stakeholders, and potentially cause financial repercussions, thereby culminating in a business crisis. Conversely, a commendable corporate governance framework integrates principles of accountability, signifying the company's cognizance of the repercussions of its decisions on each stakeholder, inclusive of employees and shareholders. Consequently, the company is duty-bound to orchestrate its choices in a manner conducive to fostering sustainable progress and enduring development [22], [23].

IT Governance

Within the ambit of corporate governance, an instrumental subset pertains to IT governance, which distinguishes itself by its exclusive focus on the information technology sector within an organization [24]. In practical terms, this entails activities encompassing the establishment of performance metrics and objectives, maintenance of technical documentation, undertaking audits, scrutinizing knowledge deficiencies, and

implementing mechanisms for monitoring progress [25]. Figure 3 delineates the five domains underpinning the framework of IT governance [26], [27].

Figure 6.3 - How the IT governance is divided.

- **Value delivery:** This domain concentrates on the efficient provision of IT advantages to other functional areas within the organization.
- **Risk Management:** This facet is dedicated to the systematic identification, communication, and judicious mitigation of risks associated with IT operations.
- **Strategic alignment:** This domain scrutinizes the congruence between the objectives delineated by the IT function and those of the broader organizational framework.
- **Resource Management:** This area is centered on the appraisal of the appropriate and effective management of information technology resources.
- **Performance Management:** This domain is concerned with the assessment of the efficacy and proficiency in which IT operations are executed.

Implementing IT governance is initially driven by the objective of fostering enhanced collaboration between business and IT sectors. It is estimated that proficient adoption of IT governance can lead to a potential increase of approximately 20% in profits due to improved alignment and delineation of responsibilities [28].

In the realm of RPA, the expansion of robotic entities necessitates meticulous implementation and maintenance, underscoring the imperative of sound governance for efficacy and objective attainment. Given the multifaceted impacts of RPA across various business domains, a well-defined framework and delineation of responsibilities are imperative. Different governance models must be considered respecting organizational conditions, resources, infrastructure, and objectives. The decentralized model, affording

greater flexibility, is recommended for companies with extensive RPA experience, fostering innovation. Conversely, the centralized or federated model, conducive to risk mitigation through systematization and standardization, is better suited for enterprises still in the nascent stages of RPA adoption [29], [30].

A notable case study involving Nordea Bank demonstrates a balanced approach, employing a centralized Center of Excellence (CoE) for most RPA-related matters, while distributing responsibilities among various operational units [7]. The federated model presents an alternative, harmonizing the CoE with autonomous business unit initiatives, thereby promoting deliberation and priority-setting, and excelling in standardization of automation and best practices [31], [32].

The Center of Excellence (CoE) emerges as a pivotal governance mechanism within organizations, pivotal in guiding the design, development, and upkeep of bots [33]. As RPA proliferates, a CoE, comprising a diverse team, is instrumental in setting policies and standards to ensure adherence to best practices [14], [29]. Its implementation entails a strategic investment, consolidating responsibilities and expertise from diverse sectors. The CoE assumes responsibility for the administration, licensing, and maintenance of RPA. Collaborative efforts under the aegis of the CoE lead to a degree of functional standardization across various sectors. Additionally, the CoE plays a vital role in change management, integration with IT, and the dissemination of RPA practices. The nature of governance may manifest through either a federated or centralized CoE, contingent on organizational structure [34].

A centralized CoE consolidates RPA functions within the organization, but may incur a concentration of efforts, potentially leading to productivity bottlenecks. Conversely, the federated model distributes responsibilities and bot management to individual business units, facilitating departmental access to CoE support [34]. In this context, the CoE assumes the role of a hub driving high-impact activities aligned with the objectives of a particular organizational unit or department, encompassing research, innovation, and technology adaptation [12].

The establishment of a CoE is also geared towards mitigating implementation-associated risks, including erroneous process selection for automation due to inadequate expectation analysis. A proof of concept is recommended to validate anticipated benefits. Risks may also arise from modifications and updates, incurring time and financial costs. Moreover, without comprehensive documentation, the organization risks losing critical process knowledge over time [12].

Exemplary RPA implementations feature a dedicated CoE, tasked with realizing proposed objectives. By operating across various organizational domains to identify, prioritize, and oversee RPA development, the CoE is instrumental in enabling scalable and risk-averse RPA adoption. *OptumServe's* implementation of a CoE exemplifies this success, culminating in a substantial increase in automation capabilities, garnering industry recognition for outstanding competency development [35].

3. Research Methodology

3.1. Multivocal Literature Review

A Multivocal Literature Review (MLR) bears resemblance to a Systematic Literature Review (SLR) in its objective to encompass both formal and informal information sources. Academic writing constitutes the primary mode of discourse within scholarly domains, whereas grey literature (GL) comprises a diverse array of information not originating from academic channels and is devoid of conventional quality control measures such as pre-publication peer review [36], [37].

In the context of this study, an extensive literature review was conducted, grounded in domain-specific expertise. The adoption of an MLR approach was deemed most capable due to the emerging nature of the subject matter, which precludes a comprehensive body of formally published literature. As elucidated earlier, the MLR integrates elements of both Systematic Literature Review and Grey Literature Review, the latter of which encompasses less formalized sources including online posts and blogs [36], [38].

Figure 4 below delineates the interrelation among SLR, GLR, and MLR. The initial component was scrutinized within designated databases, while the latter was pursued through Google Search, respectively.

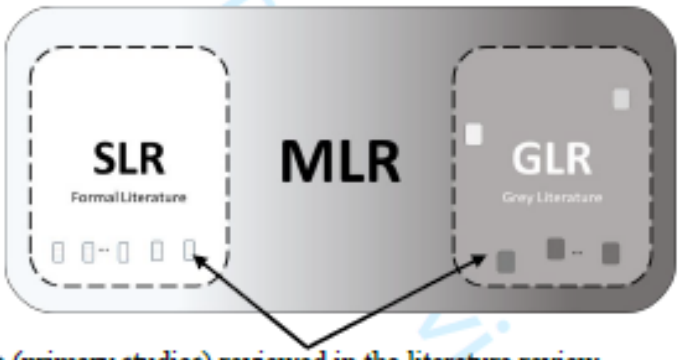


Figure 6.4 - Venn diagram showing the relationship of SLR, GLR and MLR studies.

The objective is to scrutinize the findings of the Multivocal Literature Review (MLR) in order to attain a thorough comprehension of the interplay between RPA and Governance. Specifically, the study aims to:

- Interrogate the correlation between RPA governance and its integration with Business, Information Technology (IT), and Human Resources, while also elucidating its interface with audit protocols and organizational policies as evidenced in the scrutinized documents.

Table 1 delineates distinctions between "White" literature, "Grey" literature, and "Black" literature, and delineates pertinent publication selection criteria for each category.

Table 6.1 - Distribution between "white", "Gray" literature and "Black" literature.

White literature	Grey literature	Black literature
Conference	White paper	Concepts
Papers published in journals	Blogs	Ideas
Books	Lectures	Thoughts
	Audio-video media	
	Preprints	
	Data sets	
	e-Prints	

The MLR can be divided into three parts, first the planning, then the conduction and lastly the reporting as shown in **Error! Reference source not found.** .

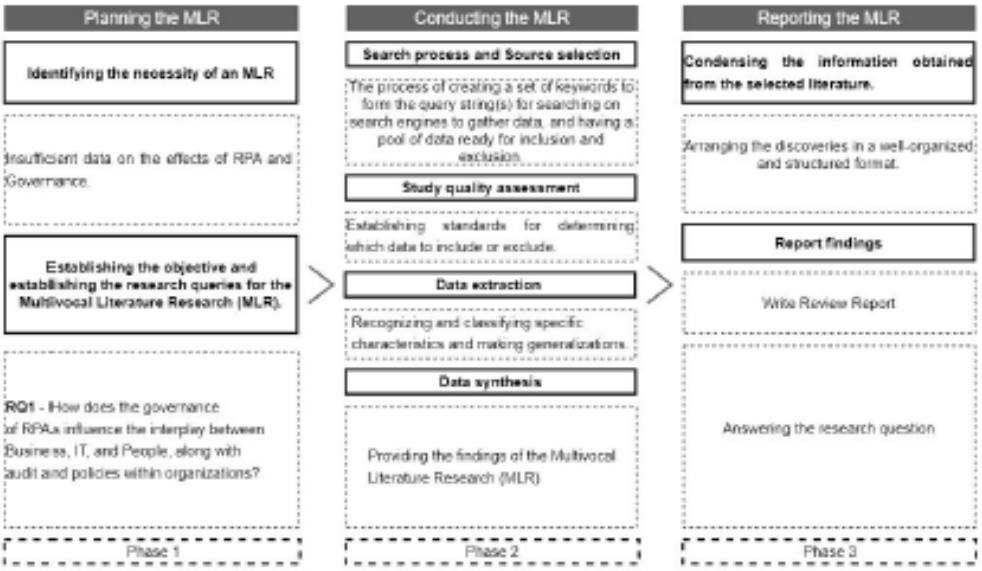


Figure 6.5 - Phases adopted in this research (adapted from [39]).

The initial phase, denoted as "Planning the Multivocal Literature Review (MLR)," comprises two pivotal steps:

- Discerning the imperative for conducting an MLR on the specific subject matter.
- Formulating the overarching objective and delineating research questions (RQs) to guide the MLR.

The subsequent phase, "Conducting the MLR," encompasses five distinct sub-stages:

- Search and Selection: This involves the formulation of a set of keywords that encapsulate the primary objectives of the study.
- Quality Assessment: It entails the critical evaluation of the credibility and objectivity of selected sources.
- Data Extraction: This step involves the retrieval of pertinent data from the identified studies.
- Data Synthesis: Here, the collated data is combined and analysed in a manner that facilitates the comprehensive addressing of the research question(s).

The concluding phase, "Reporting the MLR," often encounters challenges analogous to those encountered in the guidelines delineated for executing a Systematic Literature Review (SLR) as outlined by Kitchenham and Charters [37].

3.2. Planning the MLR

3.2.1. Review Protocol

The research was undertaken with the objective of gathering a comprehensive body of information. The subsequent selection of datasets is outlined below for reference and scrutiny:

Search string

- ("Robotic Process Automation" OR "RPA" OR "Robotic Automation") AND (Governance OR Audit OR Policies)

Datasets

- ACM Digital Library (https://dl.acm.org).
- Scopus (https://www.scopus.com/home.uri)
- EBSCO Information Services (http://search.ebscohost.com/)
- Scholar (https://scholar.google.com/)
- Google Search (https://www.google.com/)

While the utilization of Google search may be perceived as a potential limitation due to its inherent variability, it is acknowledged by certain scholars that variations in search methodology are not uncommon. Hence, it is imperative to construct a compelling rationale rather than relying solely on a singular search approach [42]. Research activities should adhere to systematic methodologies, with preference given to established search engines such as Google. Moreover, it is advisable to extend the scope of inquiry beyond the initial pages of results, considering a diverse array of sources to ensure a comprehensive review [39], [43].

3.2.2. Selection of studies

This constitutes the second phase, denoting the methodology employed in the review process. The research procedure entailed an extensive exploration of databases, followed by the judicious selection and extraction of pertinent data, which were subsequently subjected to comprehensive analysis.

In the initial stage, a systematic search was conducted in prominent academic databases. Stringent filters were applied to exclusively include peer-reviewed publications from reputable journals and academic articles. This pivotal step, delineated in Table 2, forms an integral part of the meticulous process involving the selection and scrutiny of documents, all of which must adhere to the predetermined inclusion/exclusion criteria.

In the pursuit of grey literature (GL), an analogous method was implemented. Following the execution of targeted searches using a specific "string" on the Google search engine, attention was directed towards the initial 14 pages of results. Notably, this process

entailed the exclusion of advertisements, service sales pages, subjective opinions, and non-authoritative commentaries.

3.2.3. Study quality assessment

The selection criteria, elucidating the parameters governing the inclusion or exclusion of items, are explicated and delineated in Table 2.

Table 6.2 - Inclusion/Exclusion criteria used.

Include criteria	Exclusion criteria
Related to main keywords. Documents are written in English. Filtering the search results to only show the first 14 pages from Google Search. Abstract	Not related to RPA and Governance Documents are written in a language other than English. Notifications from vendors about tools that have been excluded.

3.2.4. Data extraction

Figure 6 represents the collection process done in October 2022, showing the distinct filters used to synthesize the MLR.

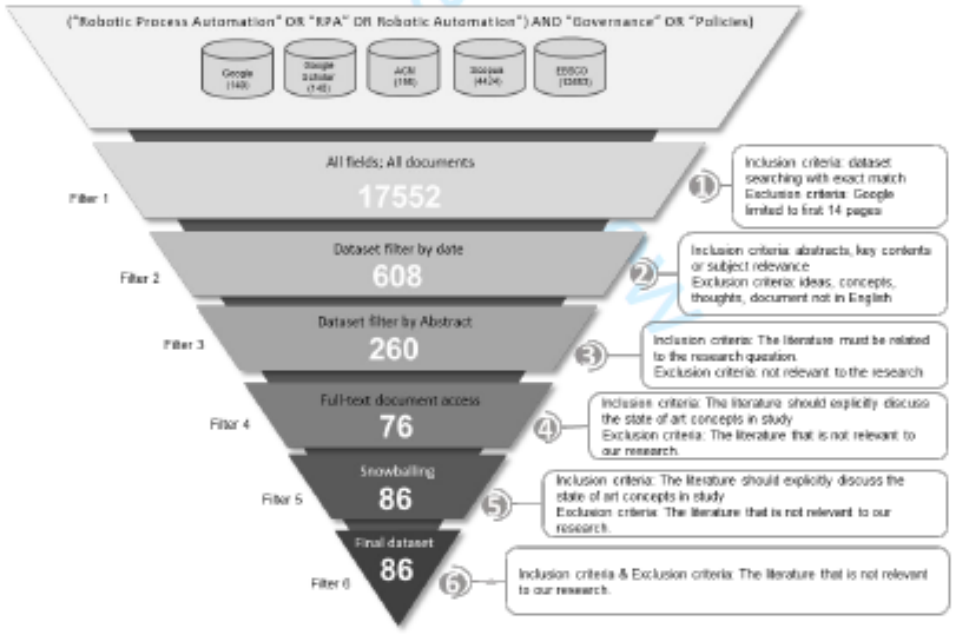


Figure 6.6 - MLR filters used (adapted from [39]).

Starting with Filter 1, an extensive exploration was conducted in "full text," examining the initial 14 pages on both Google and Scholar. Following this, Filter 2 was implemented, confining the search to "abstracts" and restricting consideration to

documents presented in the English language. Subsequently, a thoughtful manual filtration was executed to discern documents resonant with the study's thematic focus, while simultaneously eliminating any redundant entries.

To fortify the inclusivity of pertinent sources, a snowballing strategy was deployed. This method involved an accurate inspection of the reference lists of selected articles, with due diligence given to related citations [44]. This iterative process was instrumental in ensuring the incorporation of meticulously selected and academically substantive sources for the study.

4. Reporting the MLR

This section provides a comprehensive account of the research findings pertaining to the interplay between the governance of RPA and their integration with Business, IT, and People, in conjunction with their alignment with audit processes and policies. RPAs, denoting software solutions engineered to automate repetitive tasks, have emerged as a pivotal technological advancement in contemporary organizational settings [15], [45]. These software bots are endowed with user credentials, akin to those of human operators, enabling them to perform tasks with requisite permissions. Given the rapid integration of RPA in corporate operations, the governance of RPA initiatives has emerged as a pressing and significant area of scholarly inquiry [46].

Governance, in a broader context, encompasses the mechanisms and frameworks that dictate the control, organization, and management of organizations or systems. It encompasses vital components such as risk management, formulation of policies, establishment of standards, and delineation of responsibilities within various contexts, be it within business enterprises, non-profit entities, or even informal settings [47]. As depicted in Figure 7, governance assumes a foundational role, overarching and influencing the various facets under its purview. This underlines its pivotal significance in the organizational landscape.

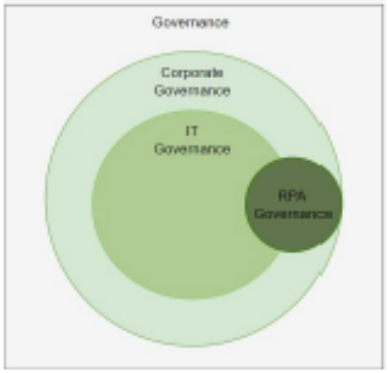


Figure 6.7 - Relationship between governances.

Corporate governance, a subset of governance, pertains to business organizations and the systems and processes governing them, with the aim of striking a balance and attaining the objectives of stakeholders, notably shareholders [47]. IT governance, in turn, is a subset of corporate governance, focusing on the oversight of technology within an organization to ensure that processes, systems, and technological components align with

established goals and standards [48]. By adhering to IT governance, it contributes to the broader objectives of corporate governance.

Within this framework, RPA governance can be considered a subset of both corporate and IT governance. It encompasses the institution's policies and processes, aiming to be accountable to all involved parties. In the context of IT governance, it entails the selection, development, security, and management of robots [49]. Effective collaboration between the IT and business sectors is advisable, even if structural governance changes are required to achieve this synergy.

RPA Governance involves various aspects, including rule implementation, leadership, and strategic planning. While RPAs can be developed without highly technical components, challenges arise when orchestrating processes across the organization, scaling them appropriately, and ensuring proper design and sizing [50].

Furthermore, RPA governance plays a crucial role in several key areas:

- Business Continuity: RPA's adaptability was highlighted during the COVID-19 pandemic, enabling organizations to maintain operational continuity even as employees transitioned to remote work [8], [39], [41], [51].
- Security: It encompasses defining roles and responsibilities, establishing security policies, and adopting guidelines to safeguard RPA systems and data [7], [8], [18], [41], [46], [51]–[56].
- Viability and Scalability: It addresses investment evaluation, resource allocation, and cost assessment, while also ensuring that RPA systems can expand and adapt in tandem with organizational growth [18], [41], [46], [56]–[58].

The subsequent analysis of selected articles led to the generation of Table 3, which highlights the most salient topics from the examined literature. Each theme is associated with corresponding articles, whether discussed in results sections, discussions, or within the broader context of the articles [59].

Table 6.3 - Findings related to the research.

MLR Findings	
Integration between business and IT	[1], [2], [7], [18], [40], [41], [45], [46], [48]–[51], [53], [54], [56], [59]–[64]
Standardization of processes	[1], [2], [7], [15], [45], [46], [51], [54], [58], [59], [65]–[71]
Compliance and risk management	[2], [7], [8], [18], [39], [41], [46], [50], [65]–[70], [72]–[83]
Employee engagement, changes in roles, responsibilities, and change management	[1], [2], [7], [8], [39], [41], [46], [47], [50], [51], [54], [59], [65], [67]–[69], [72], [73], [79], [84]

Integration between business and IT:

RPA falls under lightweight IT, requiring minimal programming skills and simplifying development. This empowers business departments to be actively involved in automation. Conversely, heavyweight IT is typically centralized and led by IT professionals.

Governance models (centralized, decentralized, federated) must align with a company's characteristics. Centralization prevents "shadow IT" but may raise concerns about process prioritization. Decentralization empowers various parties in decision-making, potentially leading to process standardization challenges. Federated governance combines elements of both models, allowing autonomy while collaborating on collective goals.

Standardization of processes:

Companies must choose processes for automation carefully, considering structured data suitability. For example, Nordea Bank emphasizes processes with stable systems and structured data. Although software can handle unstructured data with OCR, structured data is preferable to avoid high costs and errors. The choice of processes can be influenced by IT departments lacking business understanding (centralized model) or insufficient technical skills (decentralized model).

Compliance and risk management:

Integrating RPA in auditing, as seen in companies like Deloitte and Kira Systems, enhances efficiency and effectiveness. RPA minimizes time spent on routine tasks, allowing auditors to focus on high-priority activities, thus reducing errors and improving quality. It also enables the reengineering of audit processes.

The AICPA and PCAOB standards aim to control audit quality compliance, necessitating in-depth RPA-level studies. Small and medium-sized audit firms face challenges in data gathering due to diverse system formats, leading to resource-intensive processes. Effective planning and an organizational framework with defined privileges and vulnerability management are crucial for risk reduction.

Employee engagement, changes in roles, responsibilities, and change management:

While RPAs perform defined tasks, employees may still face job displacement fears. Employers can benefit from reduced costs by prioritizing less mechanical, value-added work and reallocating resources. Governance should address these concerns, providing training and opportunities for effective collaboration between robots and workers. Taxation considerations may arise, given the potential cost savings of using robots.

Roles and responsibilities need reevaluation as tasks transition from human to machine execution. Figure 8 illustrates the integrated governance approach, encompassing IT and RPA governance, process integration, compliance, risk management, and people management.

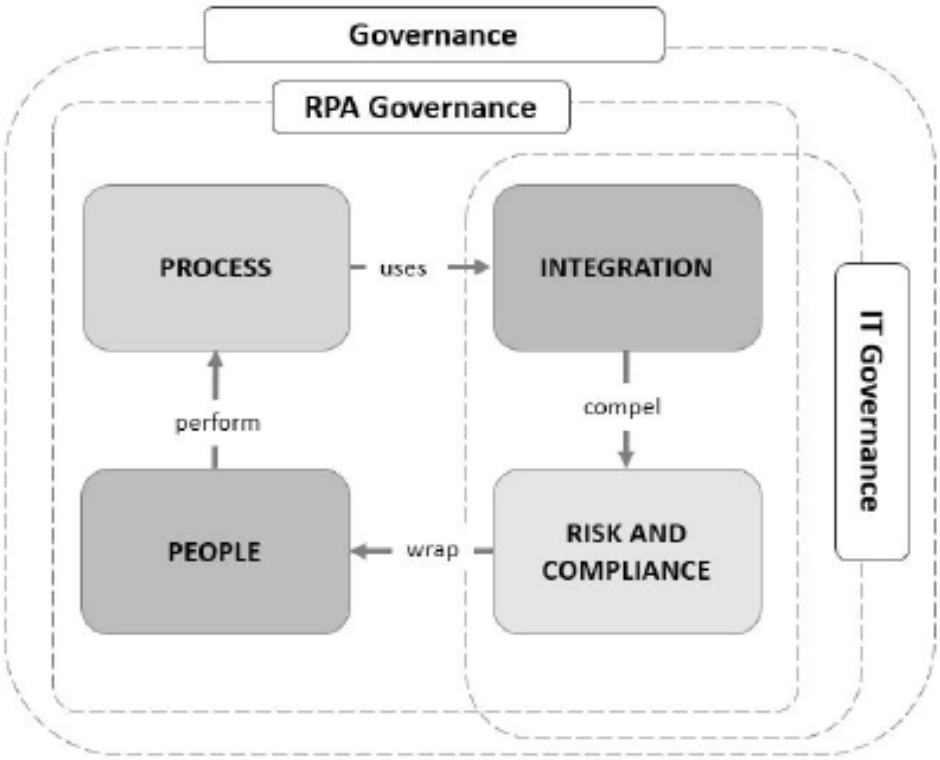


Figure 6.8 - Relationship between topics.

5. Demonstrating and evaluation

Quantitative research employs statistical tests to validate and substantiate findings, while qualitative research delves into direct experiences for a deeper and more comprehensive understanding. It encompasses values and motivations, moving beyond numerical analysis [85].

Qualitative research, conducted through interviews, aims to capture facets of the human experience [86]. This method facilitates gathering information directly from the source, providing a detailed exploration of topics, and understanding the perspectives and experiences of the interviewees. It's crucial to plan and adapt interviews to align with research questions and validate information uncovered during the study [85].

The literature review served as a foundational understanding of the subject, informing the formulation of interview questions. A questionnaire was then developed to guide the interviewer in collecting responses during the interviews. The interviewees were selected and contacted before the interviews were conducted, both via Zoom and in person.

The semi-structured interviews were designed with open-ended questions based on the literature from the MLR, aiming to capture experiences, feedback, narratives, diverse perspectives, and contextual information. This method allows flexibility, enabling a thorough exploration of topics and enriching the study with nuanced insights [86].

5.1. Population and sample

To facilitate the interviews, participants were drawn from various sectors, including business clients, the IT team overseeing robot development, the process analysis team, individuals unfamiliar with RPA, and those who engage with the outcomes produced by RPAs.

The preeminent approach for data acquisition in qualitative research is through interviews, which find applicability across various philosophical paradigms, including positivist, interpretive, and critical orientations (Myers and Newman, 2007). Within qualitative inquiry, the interview emerges as a particularly effective mechanism for data procurement (Myers and Newman, 2007) [89]. Myers (2013) further asserts that interviews afford the opportunity to elicit valuable insights from individuals occupying diverse roles and contexts [90]. Consequently, interviews represent a fitting methodological choice for the development and evaluation of an artifact. Consequently, this article will employ semi-structured interviews as the means of data collection.

A total of thirty-one individuals were interviewed, contributing their valuable experiences and insights to the research. Those not directly involved with RPA offered a unique perspective, providing viewpoints from individuals without hands-on experience with the subject or from those who interact with the results produced by the robots.

5.2. Data Collection

Initially, a document was prepared to provide the interviewees with context regarding the research and its findings, ensuring they comprehended the purpose of the interview. Subsequently, the interviews were conducted individually using the Zoom video conferencing platform or in face-to-face settings. Throughout the interviews, the interviewer recorded the responses, utilizing a pre-constructed form containing all the designated questions for the interviewees (https://forms.gle/VSqzZ4fFrtb2MLuS8).

It is important to note that the questions gathered and stored did not include any personal information, such as names or company details, to maintain the confidentiality and anonymity of the interviewees and their respective organizations. The interviewee information is outlined in Table 4, while the detailed data, organized by interviewees, is presented in Appendix A.

Table 6.4 - Information about the interviews.

Rational	Indicators				
Work Experience	0 – 5 years	5 – 10 years	10 – 15 years	15 – 20 years	> 20 years
	54.8%	16.1%	3.2%	3.2%	22.6%
Responsibility	Developer	Business Analyst	Manager	15 – 20 years	Other
	81,8%	9,1%	0%	4,5%	4,5%
Work Experience in RPA/IPA	None	5 – 10 years	10 – 15 years	15 – 20 years	> 20 years
	87.1%	12.9%	0%	0%	0%

Rational	Indicators			
Number of RPA processes	None	1 – 5 years	5 – 10 years	> 10 years
	29%	12.9%	67.9%	48.4%
Area	Business	IT	Other	
	12.9%	67.7%	19.3%	
Do you have projects at your organization?	Yes		No	
	83.9%		20%	
If not, would you feel threatened if the company decided to implement it?	Yes		No	
	16.1%		80%	

6. Results and Discussion

The process of analyzing interview data commenced with a thorough examination of the transcribed content. This involved a systematic categorization based on shared concepts, akin roles, levels of experience, and the specific area in which the interviewees were employed.

To enhance the credibility of the study, various measures were implemented. Purposive sampling was employed, allowing the researcher to pre-define participants with diverse roles, which subsequently provided a rich and varied array of information. Moreover, a pilot study involving a group of five individuals was conducted to refine the approach, diction, and interpretations employed during the interviews.

Source triangulation further bolstered the credibility by ensuring data collection from a diverse set of interviewees, some of whom were affiliated with different organizations. This facilitated a comprehensive comparison of perspectives. Additionally, iterative questioning was integrated throughout the interviews, permitting the revisiting of questions and the contextual placement of responses to potentially uncover inconsistencies.

Member checking, a vital component of the process, entailed recording the interviewee's statements and subsequently validating them to ensure their accurate representation of the interviewee's beliefs. This process also provided an opportunity for interviewees to append or amend any additional information.

The extensive process of data analysis encompassed the meticulous organization of the accumulated data, thereby facilitating subsequent interpretation based on discernible categories and shared ideas. Following this, the identification of recurring patterns, keywords, and concepts was conducted among the respondents. A narrative was subsequently constructed, rooted in the experiences relayed by the interviewees. Finally, after traversing through these meticulous steps, the results were presented in a lucid and precise manner.

Table 4 provides an overview of the responses obtained from the semi-structured interview's initial questions, aiding in the characterization of each interviewee based on factors such as years of experience and roles. Meanwhile, Table 5 offers a condensed representation of the data pertaining to the closed-ended questions posed to the

interviewees. The detailed individual responses contributing to these percentages are available in Appendix A.

Table 6.6 - Summary of closed-ended responses.

Question	Yes (%)	No (%)
Do you think that there should be integration between business and IT?	100	0
Do you think there could be issues if the process is solely defined by the business side or solely by the IT side without following a standard?	100	0
From your perspective, what is the meaning of a careful selection of processes to be automated in RPA?	-	-
Since there are no taxes on robots, but there are many on people if you were a business owner, would you prefer to retain and prioritize people over replacing them with robots for economic reasons?	3.2	96,8
Do you think RPA helps or replaces employees?	100	0
Do you believe that all individuals involved in the same project should have the same levels of permissions?	35,4	64,5
In your opinion, is understanding and preparing employees important for reducing compliance risks in RPA?	-	-

For ease of reference in subsequent discussions, Table 6 offers a condensed summary of the results resume of the topics found. More comprehensive responses can be referenced in detail in Appendix A.

Table 6.5 - Results resume with major topics found.

Questions	Resume of major topics found
Q1 - Do you think that there should be integration between business and IT?	• Alignment of goals • Process quality • Error reduction •Communication • Definition of responsibilities • Documentation
Q2 - Do you think there could be issues if the process is solely defined by the business side or solely by the IT side without following a standard?	• Knowledge limitations • Errors • Ambiguity • Resource wastage • Overload • Misalignment of objectives
Q3 - From your perspective, what is the meaning of careful selection of processes to be automated in RPA?	• Efficiency • Error Minimization • Stability • Viability
Q4 - Since there are no taxes on robots, but there are many on people, if you were a business owner, would you prefer to retain and prioritize people over replacing them with robots for economic reasons?	• Time Reduction • Mitigating Human Error • Profit • Efficiency • Essential Collaborators • Reallocation

Questions	Resume of major topics found
	• Cost Reduction
Q5 - Do you think RPA helps or replaces employees?	• Organizational Objectives • Workload • Replacement • Reallocation
Q6 - Do you believe that all individuals involved in the same project should have the same levels of permissions?	• Hierarchy • Separation of Functions and Responsibilities • Security • Project Management
Q7 - In your opinion, is understanding and preparing employees important for reducing compliance risks in RPA?	• Training and awareness • Motivation • Risks and impacts

The following section presents a series of interview questions along with a compilation of responses provided by the interviewees. These responses serve to elucidate the concepts introduced earlier, providing a more comprehensive understanding:

Q1) "Do you think that there should be integration between business and IT?"

All interviewees unanimously emphasized the necessity of integration between business and IT in the context of Robotic Process Automation (RPA). The points highlighted during the interviews to underscore the significance of collaboration between these two domains are as follows:

- Alignment of Goals: When implementing RPA, organizations have specific objectives such as cost reduction, enhanced efficiency, and improved product or service quality. Ensuring that IT and business departments comprehend each other's needs and priorities is crucial to achieving these goals.
- Process Quality: Collaboration between business and IT enables the identification of potential failures and the implementation of necessary solutions, drawing on the business's knowledge of planning requirements and customer expectations, coupled with IT's technical expertise in handling exceptions and maintenance.
- Error Reduction: Working in tandem, business and IT gain a more precise understanding of error locations, as the business possesses extensive process knowledge. This collaboration allows for the definition of process requirements and validation of business rules, preventing redundancies and implementation failures.
- Communication: Effective communication is vital for mutual comprehension of objectives and for swiftly rectifying errors. Adequate communication ensures that issues are identified and addressed promptly and efficiently.
- Definition of Responsibilities: Well-defined responsibilities prevent errors and ambiguities. Changes to processes and definitions should involve consultation with all relevant parties from both business and IT to avoid potential short or long-term impacts.
- Documentation: Comprehensive documentation serves as a record of process information, facilitating planning, understanding, change control, and version management. It grants all stakeholders, from both business and IT, insight into process operations.

In summary, IT contributes expertise in technology, implementation, and maintenance, while business areas provide knowledge of processes, requirements, and rules. Together, these areas significantly enhance the likelihood of process success.

Q2) "Do you think there could be issues if the process is solely defined by the business side or solely by the IT side without following a standard?"

All interviewees expressed concern about processes being solely defined by either the business or IT, without adhering to a standard. The identified challenges included:

- Knowledge Limitations: Sole reliance on one party may lead to gaps in understanding of business rules, requirements, implementation, testing, and integration, potentially resulting in processes that fail to achieve their objectives.
- Errors: Various errors may occur due to oversight in requirement gathering, negligence during implementation, and inadequate testing.
- Ambiguity: Processes defined by a single party may introduce ambiguity, complicating interpretation and implementation.
- Resource Wastage: Processes managed exclusively by either business or IT can result in wastage of time, money, and employee effort, particularly in cases where a robot is implemented but fails to deliver anticipated returns.
- Overload: Lack of collaboration can lead to an overload on one of the parties, resulting in inefficient resource allocation, delays, and decreased efficiency.
- Misalignment of Objectives: Synchronization between business and IT is crucial for achieving objectives. If a process is solely defined by one side, not all interests and knowledge will be leveraged, potentially undermining process execution.

Q3) "From your perspective, what is the meaning of careful selection of processes to be automated in RPA?"

The interviewees emphasized the critical importance of carefully selecting processes for automation. Several considerations were outlined:

- Efficiency: Selecting the right processes for automation is crucial to saving resources such as time and money. Processes that are repetitive and rule-based are particularly suitable.
- Error Minimization: Processes that generate frequent known errors can benefit from RPA implementation, as it can reduce execution time and mitigate errors.
- Stability: When choosing a process for automation, stability of the programs used by the robot is paramount. Ensuring that requirements and rules are well-understood, alongside technical stability, is essential for successful automation.
- Viability: An in-depth analysis should be conducted to determine if automation makes sense for each process, factoring in factors like expected return, implementation cost, maintenance, time, and effort. The focus should be on quality rather than volume, as choosing the wrong processes can lead to resource loss.

As an illustrative example, one interviewee highlighted a banking scenario. The bank had access to a list of customers with flagged credit card transactions. Automating the resolution of legal actions related to these cases was crucial to preventing long-term financial impacts and safeguarding the bank's reputation.

Q4) "As there are no taxes on robots, but there are many on people, if you were a company owner, would you prefer to retain and prioritize people over replacing them with robots for economic reasons?"

When asked about the preference between retaining and prioritizing employees over replacing them with robots for economic reasons, the responses were varied. 35.4% of the interviewees expressed a preference for retaining employees, while 64.5% leaned towards prioritizing automation. The following points were raised:

- Time Reduction: RPA can operate around the clock, significantly reducing process execution time compared to human counterparts.
- Mitigating Human Error: Robots operate based on rules, minimizing the potential for human error caused by factors such as lack of concentration or inadequate process understanding.
- Profit and Efficiency: RPA's ability to handle large volumes of information quickly can lead to increased efficiency, reduced errors, and ultimately, higher profits.
- Essential Collaboration: Certain employees play pivotal roles in processes that require human intervention, such as analysis or maintenance.
- Reallocation: Employees can be reallocated to roles demanding critical thinking and analysis, with appropriate training to equip them for these functions.
- Cost Reduction: Both the continuous operation of robots and the potential reduction of personnel can lead to cost savings, encompassing salaries, healthcare expenses, and taxes.

Ultimately, 100% of the interviewees converged on the understanding that prioritizing automation for repetitive tasks, while reserving specialized personnel for critical roles, was the optimal approach.

Q5) "Do you think RPA helps or replaces employees?"

All interviewees concurred that RPA does not wholly replace humans, but rather, it assists them. The following observations emerged:

- Organizational Objectives: Depending on the organization's goals, reducing employees may be a consideration for factors such as cost savings. Conversely, other objectives may emphasize reallocating employees.
- Workload: RPA's implementation for repetitive tasks can free up human resources to focus on higher-value tasks, especially in organizations with high workloads.
- Potential for Replacement: In instances where a process is entirely automated without collaboration, there may be concerns about job security, potentially leading to resistance in sharing knowledge for robot construction.
- Reallocation: Some organizations have used robots to facilitate the transition of employees from repetitive tasks to more analytical roles, thereby preserving jobs.

Ultimately, whether RPA assists or replaces employees is contingent upon the organization's objectives and the nature of the processes involved.

Q6) "Do you believe that all individuals involved in the same project should have the same levels of permissions?"

A significant majority (96.8%) of the interviewees expressed reservations about granting all individuals in a project the same level of access. The following points were raised to support this stance:

- Hierarchy: Establishing designated decision-makers and supervisors is crucial for effective project management.

- Separation of Functions and Responsibilities: Clear division of tasks helps prevent errors, such as instances where unauthorized transactions occur due to missteps in environment selection.
- Security: Access to confidential data should not be indiscriminately granted, as varying levels of understanding and caution exist among employees.
- Project Management: Defined roles and responsibilities contribute to organized and secure project execution.

A small minority (3.2%) of interviewees mentioned a potential advantage in certain small projects, where granting uniform access levels could streamline work and prevent delays. However, it was underscored that all actions should always be carried out under supervision, with regulation and data encryption.

Q7) "In your opinion, is understanding and preparing employees important for reducing compliance risks in RPA?"

All interviewees (100%) emphasized the pivotal role of employee understanding in reducing compliance risks associated with RPA. The following key factors were highlighted:

- Training and Awareness: Employees need comprehensive knowledge of business operations, regulations, data handling, roles, responsibilities, and associated risks.
- Motivation: Understanding the real-world impact of processes can motivate employees to maintain a broad organizational perspective and exhibit conscientiousness.
- Risks and Impacts: Unprepared employees, with limited experience, may inadvertently introduce errors, potentially leading to the compromise of confidential data.
- Creating an environment of awareness and accountability within an organization is deemed instrumental in minimizing compliance risks, enhancing the likelihood of successful RPA implementations, and safeguarding sensitive data.

In summary, the interview findings underscored that informed employees, cognizant of the risks and benefits of their work, are essential. Errors made without an appreciation of their implications can have significant financial repercussions for the organization. The insights provided by the interviewees illuminate the multifaceted considerations surrounding RPA integration, further emphasizing the nuanced interplay between technology and human expertise in organizational contexts.

7. Conclusion

This study employs a Mixed Methods Research (MLR) approach to investigate the facets of RPA and governance, emphasizing integration between business and IT, process standardization, compliance, risk management, employee engagement, role changes, and change management.

The research reveals that cohesive integration between business and IT is pivotal for the success of RPA endeavors. It aligns objectives, enhances service/product quality, reduces errors and costs, and clarifies responsibilities, among other benefits. Regarding process selection for automation, the MLR highlights its criticality, emphasizing that RPA is most effective for structured data, repetitive tasks, and well-defined rules. Properly chosen processes can lead to increased efficiency and reduced errors.

The investigation emphasizes the importance of auditing in identifying and mitigating risks associated with RPA integration, such as unauthorized access and security concerns in virtualized environments. Hierarchical structures, role segregation, and precise role assignments are vital for informed decision-making and to prevent data breaches. Employee awareness and training play a pivotal role in cultivating a culture of conscientiousness. While RPAs excel in executing repetitive tasks, human involvement remains indispensable. The study suggests that companies can benefit from a synergy between robots and human employees. A notable limitation is the scarcity of extant literature on RPA due to its relatively recent emergence.

Future investigations might delve deeper into specific research domains, potentially encompassing longitudinal studies on organizations to offer extended insights into adaptations in RPA governance. Additionally, exploring communication processes across sectors could unveil opportunities for optimization. In-depth case studies might illuminate how companies navigate the reallocation and training of employees transitioning from repetitive tasks to diverse roles.

References

[1] R. C. Ruiz, A. J. Ramírez, M. J. Cuaresma, J. G. Enríquez, "Hybridizing humans and robots: An RPA horizon envisaged from the trenches," Computers in Industry, vol. 138, pp. 103615, Jun. 2022, ISSN 0166-3615, doi: 10.1016/j.compind.2022.103615.

[2] I. Lindgren, D. Toll, and U. Melin, "Automation as a Driver of Digital Transformation in Local Government: Exploring Stakeholder Views on an Automation Initiative in a Swedish Municipality," in ACM International Conference Proceeding Series, Association for Computing Machinery, Jun. 2021, pp. 463–472. doi: 10.1145/3463677.3463685.

[3] A. Orynbayeva, "A governance model for managing Robotics Process Automation (RPA)," Master Thesis, Delft University of Technology, Aug. 2019. [Online]. Available: http://resolver.tudelft.nl/uuid:b4609d10-9318-465c-baa4-e945e7de1a96

[4] "Robotic process automation (RPA): Potential for businesses | ALSO," accessed Jun. 12,2022.[Online].Available: https://www.also.com/ec/cms5/en_6000/6000/blog/future-technologies/robotic-process-automation-rpa-potential-for-businesses.jsp

[5] C. Boulton, "What is RPA? A revolution in business process automation," 2018. [Online]. Available: https://www.cio.com/article/227908/what-is-rpa-robotic-process-automation-explained.html (accessed Jun. 10, 2022).

[6] J. Wewerka and M. Reichert, "Robotic process automation - a systematic mapping study and classification framework," Enterprise Information Systems, Taylor and Francis Ltd., 2021, doi: 10.1080/17517575.2021.1986862.

[7] D. Kedziora and E. Penttinen, "Governance models for robotic process automation: The case of Nordea Bank," Journal of Information Technology Teaching Cases, vol. 11, no. 1, pp. 20–29, 2020, doi: 10.1177/2043886920937022.

[8] S. A. Harrast, "Robotic process automation in accounting systems," Journal of Corporate Accounting and Finance, vol. 31, no. 4. John Wiley and Sons Inc, pp. 209–213, Oct. 01, 2020. doi: 10.1002/jcaf.22457.

[9] B. L. Handoko, A. S. L. Lindawati, and M. Mustapha, "Robotic process automation in audit 4.0," in ACM International Conference Proceeding Series, Association for Computing Machinery, Jul. 2021, pp. 128–132. doi: 10.1145/3481127.3481140.

[10] W. H. Money, "Resolving Pressure and Stress on Governance Models from Robotic Process Automation Technologies," Tommy and Victoria Baker School of Business, The Citadel, Charleston, South Carolina, USA.

[11] C. Zhang, H. Issa, A. Rozario, and J. Sveistrup Soegaard, "Robotic Process Automation (RPA) Implementation Case Studies in Accounting: A Beginning to End Perspective," Accounting Horizons, vol. 37, no. 1, pp. 193–217, 1 March 2023, doi: 10.2308/HORIZONS-2021-084.

[12] P. Marciniak and R. Stanisławski, "Internal determinants in the field of RPA technology implementation on the example of selected companies in the context of industry 4.0 assumptions," Information (Switzerland), vol. 12, no. 6, Jun. 2021, doi: 10.3390/info12060222.

[13] M. Smeets, R. Erhard, and T. Kaußler, "Robotic Process Automation (RPA) in the Financial Sector," 2021, ISBN 978-3-658-32973-0 (Print), ISBN 978-3-658-32974-7 (eBook), https://doi.org/10.1007/978-3-658-32974-7.

[14] R. Syed et al., "Robotic Process Automation: Contemporary themes and challenges," Comput Ind, vol. 115, Feb. 2020, doi: 10.1016/j.compind.2019.103162.

[15] J. Chacón-Montero, A. Jiménez-Ramírez, and J. G. Enríquez, "Towards a method for automated testing in robotic process automation projects," in Proceedings - 2019 IEEE/ACM 14th International Workshop on Automation of Software Test, AST 2019, Institute of Electrical and Electronics Engineers Inc., May 2019, pp. 42–47. doi: 10.1109/AST.2019.00012.
[16] A. Sobczak and L. Ziora, "The use of robotic process automation (Rpa) as an element of smart city implementation: A case study of electricity billing document management at bydgoszcz city hall," Energies (Basel), vol. 14, no. 16, Aug. 2021, doi: 10.3390/en14165191.
[17] A. Januszewski, J. Kujawski, and N. Buchalska-Sugajska, "Benefits of and obstacles to RPA implementation in accounting firms," in Procedia Computer Science, Elsevier B.V., 2021, pp. 4672–4680. doi: 10.1016/j.procs.2021.09.245.
[18] P. Hofmann, C. Samp, and N. Urbach, "Robotic process automation," Electronic Markets, vol. 30, no. 1, pp. 99–106, Mar. 2020, doi: 10.1007/s12525-019-00365-8.
[19] M. Ali, "Governance and Good Governance: A Conceptual Perspective," The Dialogue, vol. 10, pp. 66-77.
[20] "Governance: Meaning, Definition, 4 Dimensions, And Types." https://schoolofpoliticalscience.com/definitions-and-types-of-governance/ (accessed Jul. 06, 2023).
[21] "Principles of Corporate Governance." https://corpgov.law.harvard.edu/2016/09/08/principles-of-corporate-governance/ (accessed Jul. 07, 2023).
[22] B. Lutkevich, "What is Corporate Governance?" https://www.techtarget.com/searchsecurity/definition/corporate-governance (accessed Jul. 07, 2023).
[23] "Corporate Governance." https://www.diligent.com/insights/corporate-governance/ (accessed Jul. 07, 2023).
[24] "IT Governance - Qualified Audit Academy." https://www.audit-academy.be/en/glossary/it-governance (accessed May 20, 2023).
[25] "IT Governance: Definition, Frameworks, and Best Practices." https://blog.invgate.com/it-governance (accessed May 20, 2023).
[26] M. Fletcher, "Five Domains of Information Technology Governance for Consideration by Boards of Directors," University of Oregon Applied Information Management Program, June 2006.
[27] "What is IT Governance?" https://itchronicles.com/what-is-it-governance/ (accessed Jul. 08, 2023).
[28] S. De Haes and W. Van Grembergen, "IT Governance and Its Mechanisms," 2004, Information Systems Audit and Control Association.
[29] J. Aughton and S. Ozer, "Refocus your Robotic Process Automation Lens: Internal Control over Financial Reporting (ICFR) Considerations for Developing and Implementing Bots," 2019 Deloitte Development LLC.
[30] P. L. Willcocks, M. Lacity, and A. Craig, "The IT Function and Robotic Process Automation," The Outsourcing Unit, Department of Management, The London School of Economics and Political Science, London, UK, and University of Missouri-St. Louis, St. Louis, MO, USA, October 2015.
[31] T. Kämäräinen, "MANAGING ROBOTIC PROCESS AUTOMATION: OPPORTUNITIES AND CHALLENGES ASSOCIATED WITH A FEDERATED GOVERNANCE MODEL," 2018. [Online]. Available: www.aalto.fi
[32] A. Asatiani, T. Kämäräinen, and E. Penttinen, "Unexpected Problems Associated with the Federated IT Governance Structure in Robotic Process Automation (RPA) Deployment," Department of Information and Service Management, 2019.
[33] L. Willcocks, J. Hindle, and M. Lacity, "Keys to RPA Success: How Blue Prism Clients Are Gaining Superior Long-Term Business Value," March 2019. [Online]. Available: www.knowledgecapitalpartners.com
[34] C. Flechsig, F. Anslinger, and R. Lasch, "Robotic Process Automation in purchasing and supply management: A multiple case study on potentials, barriers, and implementation," Journal of Purchasing and Supply Management, vol. 28, no. 1, Jan. 2022, doi: 10.1016/j.pursup.2021.100718.
[35] O. Serve, "Robotic Process Automation for Government (RPAG): Utilizing RPA to Advance Federal Government Functions," 2021, Optum.
[36] V. Garousi, M. Felderer, and M. V. Mäntylä, "The need for multivocal literature reviews in software engineering: Complementing systematic literature reviews with grey literature," in ACM International Conference Proceeding Series, Association for Computing Machinery, Jun. 2016. doi: 10.1145/2915970.2916008.
[37] V. Garousi, M. Felderer, and M. V. Mäntylä, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," Inf Softw Technol, vol. 106, pp. 101–121, Feb. 2019, doi: 10.1016/j.infsof.2018.09.006.
[38] G. T. G. Neto, W. B. Santos, P. T. Endo and R. A. A. Fagundes, "Multivocal literature reviews in software engineering: Preliminary findings from a tertiary study," 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Porto de Galinhas, Brazil, 2019, pp. 1-6, doi: 10.1109/ESEM.2019.8870142.
[39] J. Brás, R. Pereira, and S. Moro, "Intelligent Process Automation and Business Continuity: Areas for Future Research," Information 2023, Vol. 14, Page 122, vol. 14, no. 2, p. 122, Feb. 2023, doi: 10.3390/INFO14020122.
[40] N. E. Vincent, A. Igou, and M. B. Burns, "Preparing for the robots: A proposed course in robotic process automation," Journal of Emerging Technologies in Accounting, vol. 17, no. 2, pp. 75–91, Apr. 2020, doi: 10.2308/jeta-2020-020.

[41] Jagreet Kaur, "RPA Governance Model with Best Practices via CoE," 2021. https://www.xenonstack.com/insights/rpa-governance (accessed Jun. 10, 2022).
[42] C. Stansfield, K. Dickson, and M. Bangpan, "Exploring issues in the conduct of website searching and other online sources for systematic reviews: How can we be systematic?," Systematic Reviews, vol. 5, no. 1. BioMed Central Ltd., Nov. 15, 2016. doi: 10.1186/s13643-016-0371-9.
[43] S. Coleman, J. M. Wright, J. Nixon, L. Schoonhoven, M. Twiddy, and J. Greenhalgh, "Searching for Programme theories for a realist evaluation: A case study comparing an academic database search and a simple Google search," BMC Med Res Methodol, vol. 20, no. 1, Aug. 2020, doi: 10.1186/s12874-020-01084-x.
[44] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in ACM International Conference Proceeding Series, Association for Computing Machinery, 2014. doi: 10.1145/2601248.2601268.
[45] J. Kokina and S. Blanchette, "Early evidence of digital labor in accounting: Innovation with Robotic Process Automation," International Journal of Accounting Information Systems, vol. 35, Dec. 2019, doi: 10.1016/j.accinf.2019.100431.
[46] K. Osmundsen, J. Iden, and B. Bygstad, "Organizing robotic process automation: Balancing loose and tight coupling," in Proceedings of the Annual Hawaii International Conference on System Sciences, IEEE Computer Society, 2019, pp. 6918–6926. doi: 10.24251/hicss.2019.829.
[47] S. Ali, P. Green, and A. Robb, "Information technology investment governance: What is it and does it matter?," International Journal of Accounting Information Systems, vol. 18, pp. 1–25, Sep. 2015, doi: 10.1016/j.accinf.2015.04.002.
[48] R. Peterson, "Crafting information technology governance," Information Systems Management, vol. 21, no. 4, pp. 7–22, 2004, doi: 10.1201/1078/44705.21.4.20040901/84183.2.
[49] A. Marrella et al., "Business Process Management Blockchain, Robotic Process Automation, and Central and Eastern Europe Forum." [Online]. Available: https://link.springer.com/bookseries/7911
[50] J. May, "There can't be RPA success without RPA governance," https://blogs.mulesoft.com/digital-transformation/rpa-governance/, Jul. 29, 2022. https://blogs.mulesoft.com/digital-transformation/rpa-governance/ (accessed Jan. 28, 2022).
[51] E. Hartikainen, V. Hotti, and M. Tukiainen, "Improving Software Robot Maintenance in Large-Scale Environments–is Center of Excellence a Solution?," IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3205420.
[52] J. Johansson, M. Thomsen, and M. Åkesson, "Public value creation and robotic process automation: normative, descriptive and prescriptive issues in municipal administration," Transforming Government: People, Process and Policy, 2022, doi: 10.1108/TG-11-2021-0193.
[53] S. Hegde, S. Gopalakrishnan, and M. Wade, "Robotics in Securities Operations," Journal of Securities Operations & Custody, vol. 10, no. 1, January 1, 2018.
[54] K. C. Moffitt, A. M. Rozario, and M. A. Vasarhelyi, "Robotic process automation for auditing," Journal of Emerging Technologies in Accounting, vol. 15, no. 1. American Accounting Association, pp. 1–10, Mar. 01, 2018. doi: 10.2308/jeta-10589.
[55] M. Joana, "There Can't Be RPA Success Without RPA Governance," https://blogs.mulesoft.com/digital-transformation/rpa-governance/, accessed Nov. 19, 2022.
[56] V. Kumar, "Integration of Robotic Process Automation (RPA)," May 5, 2022, [Online]. Available: https://univdatos.com/integration-of-robotic-process-automation-rpa/. (accessed: Jun. 07, 2023).
[57] R. Chugh, S. Macht, and R. Hossain, "Robotic Process Automation: a review of organizational grey literature," International Journal of Information Systems and Project Management, vol. 10, no. 1, pp. 5–26, 2022, doi: 10.12821/ijispm100101.
[58] F. Huang and M. A. Vasarhelyi, "Applying robotic process automation (RPA) in auditing: A framework," International Journal of Accounting Information Systems, vol. 35, Dec. 2019, doi: 10.1016/j.accinf.2019.100433.
[59] A. Dahiyat, "ROBOTIC PROCESS AUTOMATION AND AUDIT QUALITY," Corporate Governance and Organizational Behavior Review, vol. 6, no. 1, pp. 160–167, 2022, doi: 10.22495/cgobrv6i1p12.
[60] "RPA in Audit: 7 insights I wish I had when building RPA solutions." https://blog.datasnipper.com/rpa-in-audit-insights (accessed Jun. 07, 2023).
[61] R. Ali, "Incorporating Robotic Process Automation (RPA) Capability in Internal Audit," LinkedIn, Feb. 2020, [Online]. Available: https://www.linkedin.com/pulse/incorporating-robotic-process-automation-rpa-capability-rameez-ali/. Accessed: Jun. 07, 2023.
[62] "Generating Internal Audit Workpapers With Robotic Process Automation - CrossCountry Consulting," August, 2020, [Online]. Available: https://www.crosscountry-consulting.com/insights/blog/generating-internal-audit-workpapers-with-rpa/. Accessed: Jun. 07, 2023.
[63] "Robotic Process Automation (RPA) Powering Up the Audit," KPMG, Nov. 2021, [Online]. Available: https://kpmg.com/za/en/home/insights/2021/11/robotic-process-automation--rpa--powering-up-the-audit.html. Accessed: Jul. 03, 2023.
[64] A. S. Tommervag, T. Bach, and B. Jager, "Leveraging the competition: Robotic Process Automation (RPA) enabling competitive Small and Medium sized Auditing Firms," in 2022 IEEE/SICE International Symposium on

System Integration, SII 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 833–837. doi: 10.1109/SII52469.2022.9708789.
[65] C. Gex and M. Minor, "Make Your Robotic Process Automation (RPA) Implementation Successful," 2018, American Society of Military Comptrollers.
[66] R. Chugh, S. Macht, and R. Hossain, "Robotic Process Automation: a review of organizational grey literature," International Journal of Information Systems and Project Management, vol. 10, no. 1, pp. 5–26, 2022, doi: 10.12821/ijispm100101.
[67] "Never Compromise on RPA Governance and Compliance," Cloud4C, Nov. 2020, [Online]. Available: https://www.cloud4c.com/rpa/blogs/rpa-governance. Accessed: Jul. 03, 2023.
[68] "Governance of an RPA project – Beyond traditional project management." https://www.optum.in/thought-leadership/library/governance-rpa-project.html (accessed Jul. 04, 2023).
[69] Y. Rechtman, "Can Robotic Process Automation Improve Quality Control in Audits?" August 2021. [Online]. Available: https://www.cpajournal.com/2021/08/10/can-robotic-process-automation-improve-quality-control-in-audits/. (accessed: Jul. 04, 2023).
[70] "How do you audit a robot? | ICAEW." [Online] https://www.icaew.com/technical/internal-audit-community/internal-audit-resource-centre/how-do-you-audit-a-robot (accessed Jul. 04, 2023).
[71] "Artificial Intelligence, Robotics and Automation,", DLA Piper, 2020.
[72] "What Is Robotic Process Automation (RPA)?" https://www.microfocus.com/en-us/what-is/robotic-process-automation (accessed Jul. 04, 2023).
[73] M. Cohen, A. M. Rozario, and C. Zhang, "Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures," August 2019. [Online]. Available: http://bit.ly/2JKLCee.
[74] A. M. Rozario and M. A. Vasarhelyi, "How Robotic Process Is Transforming," 2018. [Online]. Available: https://www.uipath.com/
[75] C. Zhang, "Intelligent process automation in audit," Journal of Emerging Technologies in Accounting, vol. 16, no. 2, pp. 69–88, Sep. 2019, doi: 10.2308/jeta-52653.
[76] "RPA: First Steps to Greater Internal Audit Efficiency | Corporate Compliance Insights." https://www.corporatecomplianceinsights.com/rpa-first-steps-to-greater-internal-audit-efficiency/ (accessed Jun. 07, 2023).
[77] "Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures - The CPA Journal." https://www.cpajournal.com/2019/08/14/exploring-the-use-of-robotic-process-automation-rpa-in-substantive-audit-procedures/ (accessed Jun. 07, 2023).
[78] T. Nam, "Citizen attitudes about job replacement by robotic automation," Futures, vol. 109, pp. 39–49, May 2019, doi: 10.1016/j.futures.2019.04.005.
[79] Innovation Committee and Chief Information Officers Council, "ROBOTIC PROCESS AUTOMATION IN FEDERAL AGENCIES." [Online]. Available: https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1704350/the-bots-are-coming-robotic-process-au
[80] A. Katara and Z. Rashid, "Robotic Process Automation for Risk and Compliance," March 20, 2018. [Online]. Available: https://www.rmmagazine.com/articles/article/2018/03/20/-Robotic-Process-Automation-for-Risk-and-Compliance-. (Accessed: Jul. 04, 2023).
[81] D. Dhanashree, "The Future of RPA in Audit & Compliance," Published: Jun, 2022. [Online]. Available: https://nanonets.com/blog/rpa-in-audit-and-compliance/. (Accessed: Jul. 04, 2023).
[82] U. Aziz, "Robotic Process Automation (RPA) Audit Process Guide & Impacts," Published: August, 2022. [Online]. Available: https://linfordco.com/blog/rpa-audit-process-impact/. (Accessed: Jul. 04, 2023).
[83] M. Huettinger and J. A. Boyd, "Taxation of robots – what would have been the view of Smith and Marx on it?," Int J Soc Econ, vol. 47, no. 1, pp. 41–53, Jan. 2020, doi: 10.1108/IJSE-11-2018-0603.
[84] S. Wang, Q. Sun, Y. Shen, and X. Li, "Applications of Robotic Process Automation in Smart Governance to Empower COVID-19 Prevention," in Procedia Computer Science, Elsevier B.V., 2022, pp. 320–323. doi: 10.1016/j.procs.2022.04.043.
[85] A. Castleberry and A. Nolen, "Thematic analysis of qualitative research data: Is it as easy as it sounds?," Curr Pharm Teach Learn, vol. 10, no. 6, pp. 807–815, Jun. 2018, doi: 10.1016/J.CPTL.2018.03.019.
[86] J. Donalek, "The Interview in Qualitative Research," 2005, Accessed: Sep. 12, 2023. [Online]. Available: https://web.archive.org/web/20200321051035id_/https://www.suna.org/download/members/unjarticles/2005/05apr/124.pdf
[87] A. K. Shenton, "Strategies for Ensuring Trustworthiness in Qualitative Research Projects," Education for Information, vol. 22, no. 2, pp. 63-75, Jul. 2004. doi: 10.3233/EFI-2004-22201.
[88] L. Busetto, W. Wick, and C. Gumbinger, "How to use and assess qualitative research methods," Neurol. Res. Pract., vol. 2, p. 14, 2020. doi: 10.1186/s42466-020-00059-z.
[89] M. D. Myers and M. Newman, "The qualitative interview in IS research: Examining the craft," Information and Organization, vol. 17, no. 1, pp. 2–26, 2007, doi: 10.1016/j.infoandorg.2006.11.001.
[90] M. D. Myers, Qualitative Research in Business and Management Second Edition. SAGE Publications Ltd; Second edition, 2013.

Appendix A

#	Q1 - Do you think that there should be integration between business and IT?
1	The interviewee spoke about the importance of the union between business and IT because each one has a type of responsibility and expertise.
2	The combination of IT and Business can optimize the way business is done when compared to traditional business
3	Process should be improved collaboratively by the IT and business for greater efficiency and success.
4	There should be a balance so that both areas can contribute their specialties, increasing the quality of processes, and aiding in standardization and knowledge transfer through documentation.
5	IT is a mean to achieve business goals. So, those two sectors must be integrated, somehow.
6	Integration between the two areas is crucial as they complement each other. The business is vital in identifying processes and monitoring them, while the IT area is better suited for implementing solutions and solving technical issues.
7	An organization where IT and business strategy are in integrated can improve agility and operational efficiencies while also enterprises function better, make more profit and hit their goals with less effort.
8	Working together could reduce costs, align goals and promote process improvement
9	Important because if it's only in IT and separate from the business, it won't address the organization as a whole; it will be from a single perspective.
10	The best way would be to come together for process understanding and follow-up when it goes into production.
11	It's important because it bridges the languages of business and IT, which are different, and this translation of language is crucial for correct interpretation.
12	Certainly, the connection is critical; if there isn't that connection between the two, it can generate many risks for the organization, not just financial risks.
13	Collaboration between these two functions is very important for reasons such as alignment of objectives and effectiveness.
14	With the help of IT, the improvement and facilitation of many business processes can be achieved.
15	I know of a department that created their own robots without specialized employees, resulting in poor development and maintenance difficulties, which can harm the institution.
16	I think one doesn't exist without the other; you need the business part well defined first, and then you can have software that works well.
17	There should always be communication between the two; otherwise, it can go wrong for both sides.
18	The business understands more about the business rules, while IT is more focused on the technical aspects.
19	That's exactly what prevents errors because there is the person who develops the process and the person from the business who understands the day-to-day work to be executed.
20	One evolves with the other; if the business part doesn't work well, technology cannot execute.
21	It's important that the department also has some understanding of how the processes to be automated work in order to communicate effectively with those handling the technical aspects.
22	Collaboration between the two areas is essential, as well as clear alignment, communication, and well-defined roles and responsibilities.
23	Collaboration is necessary; those who will develop lack knowledge in the business area, and vice versa.
24	I believe that the business and IT should maintain unity, as I think it would optimize time, service, and contribute to the product's quality.
25	Both sides bring something valuable to the process. On one hand, there's business knowledge, and on the other, technical knowledge. Robots work better when both are present.
26	Collaboration between the two is important, and there should be alignment so they can work together and avoid conflicts of interest.
27	Integration between the business and IT is important because it streamlines the work of both, reducing time as each is an expert in their respective areas, and it decreases costs by preventing errors.
28	The business needs to focus on the analysis and process documentation, while IT should handle the development and maintenance of those processes.
29	Each one plays their part in the area they know best: the business side analyzes and documents processes, while IT develops, aiding in organization and preventing overload.
30	Working together, the goals are more likely to be achieved, and the union of these two areas will combine their respective strengths.
31	It's important to always have a bridge between the two areas for better understanding of the contexts each part executes. It's also essential to have someone who understands both sides to facilitate the connection between them.

#	Q2 - Do you think there could be issues if the process is solely defined by the business side or solely by the IT side without following a standard?
1	In agreement with the previous response, if each department works within its specialization, it will decrease the likelihood of errors and consequently losses to the organization.
2	The business knows how the process works and the IT knows how to implement. One without the other could lead to errors in the process or non-ideal scenarios
3	The lack of collaboration between these areas can result in unnecessary resource expenditure due to misalignment of objectives or even a lack of necessary knowledge.
4	If the process is solely defined and executed by one of the departments, errors can be made, and collaboration between them is crucial to ensure everything progresses smoothly.
5	Business side must consider IT potentialities and limitations as well IT side must know what the business goals are to focus on delivering what is required.
6	IT may need the business due to a lack of sufficient knowledge in the business area, and the business may need IT to overcome technical issues.
7	The lack of standard processes involving both areas can lead to unmet business expectations.
8	It is essential that both sides work together, follow determined processes and communicate well, to ensure that initiatives generate value for the organization.
9	Yes, because they wouldn't address the topics comprehensively.
10	There is a lack of technology knowledge, especially for maintenance if it's done solely by the business, and if done solely by IT, there would be a lack of business knowledge for automation.
11	If it were done by the business, they probably wouldn't be implemented efficiently, and if it were done by IT, the business details wouldn't be considered.
12	All the problems, primarily a waste of time and money.
13	Problems such as lack of standards, lack of alignment of objectives and inefficiency may arise.
14	It should never be defined by just one party. The business should define rules and provide examples of how the process is done manually, and IT will assess the feasibility and suggest possible step-by-step improvements.
15	The business side doesn't understand the technical aspects, and IT doesn't know how to gather requirements or manage processes.
16	The robot might not be useful in the end; it might not solve the business problem if it wasn't well-defined from the beginning or executed well.
17	A businessperson may have an easier time understanding and communicating with the client, while a developer has more knowledge of what can be done at the code level.
18	It would be much more difficult to reach the end goal as the number of processes scales up.
19	Yes, because each person has knowledge of their part, that's why there should be a union between the two.
20	The person who writes the process knows about the business logic and not about the execution part, and vice versa.
21	On the IT side, people may not have a complete understanding of the process, and on the business side, they may not have a complete understanding of the tools.
22	The combination of both areas is an asset, merging business knowledge with IT expertise.
23	IT may not know how to gather the process correctly, and the business side may not develop as efficiently.
24	IT without full knowledge of the business and the business without full knowledge of IT could lead to a series of errors.
25	If only IT handles everything, the business knowledge will be missing, and if it's solely the business side handling it, they might not do it as efficiently, potentially not saving the money and time intended.
26	The business side wouldn't be able to provide the necessary maintenance and effective development, whereas the IT side may not understand the business's gains and losses. Each area has its focus, and their union is ideal.
27	There needs to be unity so that the IT department can complement the knowledge of the business area.
28	the business may not possess as much technical knowledge, which could lead to errors or process inefficiencies. Conversely, a developer without business knowledge would struggle to analyze the necessary or unnecessary steps in building a process.
29	Overloading, as the business may not know how to develop and maintain processes, and IT may not understand the business enough, leading to future problems.
30	It can bring problems like a lack of specialized knowledge, which can translate into significant business impacts.
31	Handling processes individually can lead to limited knowledge, a lack of effective documentation, and communication with the potential for negative impacts.

#	Q3 - From your perspective, what is the meaning of careful selection of processes to be automated in RPA?
1	Processes that don't require human critical thinking and accurate choices save time and money.
2	Processes need to be repetitive for maximum optimization, and making the wrong choice can lead to future losses.
3	A process should have well-defined rules and minimal changes to prevent discontinuation or resource losses in the future.
4	RPA processes should be the ones where tasks are repetitive and follow a specific standard that is not being altered very often
5	Prioritizing the right processes ensures that RPA implementation delivers the desired benefits while minimizing potential risks and challenges.
6	The processes to be selected should add value to the company, based on well-defined and repetitive rules.
7	Carefully check the complexity, stability, scalability and importance of the process
8	Thorough analysis to select processes in line with the organization's objectives and suitable for automation, thereby increasing the likelihood of success and financial return.
9	If the right process selection is not made, there can be a loss of time in implementation, and maintenance ends up with higher costs and a greater risk of poor results.
10	The risk is to continue having people with repetitive tasks and automating processes that don't need it. Sometimes there is too much concern about the volume of automation and not enough focus on quality.
11	Processes should always have a hierarchy and consider profitability. FTEs means people are reallocated and not fired, and in FSTS cost reduction or elimination should be prioritized.
12	Adding value, a good selection increases the added value to the organization, and a poor selection is a waste.
13	Can significantly impact the success and efficiency of an implementation.
14	Automating daily and repetitive processes should involve analyzing the cost of automation, including licenses and infrastructure, when choosing a process. It's essential to balance the benefits of automation with the required investment.
15	It's very important because there are things that can meet customer expectations and others that can't, and this analysis and realism are necessary in this regard.
16	It's what solves the problem; it's better to invest in processes that can contribute than in processes that don't save as much work.
17	There should be attention in the process selection; it should be a process that saves someone's time, which can be used for more critical tasks.
18	It depends on whether the development is feasible, feasibility analysis is one of the key aspects of a process. If not done correctly, it can lead to overspending of resources.
19	Time savings, fewer errors, reduced costs, and consequently, having time for other activities that require greater human intelligence.
20	The wrong choice can generate costs, loss of time, and labor.
21	This can lead to application errors, business errors, data non-conformity errors; the processing can be done incorrectly, resulting in an unexpected outcome.
22	Loss of time, money, and resources. A process that won't yield returns is a detriment to the organization, impacting both its reputation and finances.
23	The choice of processes to be automated is those that bring time and cost savings to the organization.
24	If a process is not chosen carefully, it may lack data and knowledge about the process, which can result in a loss of time, money, and other resources.
25	They should have certain characteristics such as being repetitive and having as few special exceptions as possible to avoid resource loss.
26	If the choice is not made carefully, it can result in the loss of money and time. If the goal is to reduce time spent on repetitive tasks, selecting the wrong processes can hinder achieving that objective.
27	It can lead to errors, unnecessary time and money spent because not every process is feasible to automate. Some processes may not be repetitive, or the economic benefit for the organization may not justify automation.
28	It's essential to choose what truly needs to be automated, as otherwise, it could be discontinued for various reasons.
29	It can have an impact because the robot may not be able to do what the business requires, which can affect other areas that depend on correct execution.
30	There should be stability in the process to be automated, it must be a well-structured process, using stable applications, and estimating and analyzing the impact in terms of resource allocation is crucial.
31	The choice of a process should consider the benefits to the organization, the cost of execution, and the time saved.

#	Q4 - Since there are no taxes on robots, but there are many on people, if you were a business owner, would you prefer to retain and prioritize people over replacing them with robots for economic reasons?
1	I would prioritize the implementation of RPA, reducing process time, increasing profits, and lowering various unnecessary costs while retaining essential employees and reallocating others.
2	It mainly depends on the task. If the task is repetitive, the robot is perfect. But if there are exceptions, the human does it better
3	Robots would perform the work more efficiently and quickly, but can fail, so human oversight is necessary.
4	People must be present to maintain the robots and people offer certain skills that robots cannot mimic
5	We live in a competitive market so reducing costs without losing quality is mandatory to "survive".
6	I'd prefer robots, not only for economic reasons but also due to their greater efficiency compared to humans and I'd adapt employees to new roles integrated with RPAs.
7	This means RPA would replace humans and many would be out of a job, but as a business owner everything is a transaction so I would try to save as much money as possible
8	People need to be present to maintain the robots, and people offer specific skills that robots cannot mimic. Robots can be present in repetitive tasks, reducing possible human errors.
9	Economically, I would choose to replace people, but in other aspects, there is the analysis and evaluation of results that must be done by a human.
10	Prioritize robots, saving money and having everything done the same way, and reallocate the necessary employees to higher-value activities.
11	But there should always be a human foundation.
12	It's not about paying taxes; humans should add value and not be engaged in repetitive activities.
13	People are still needed because automatism can generate errors that have to be corrected by a human.
14	The ideal strategy would be to reduce resources per process instead of replacing them completely.
15	Economically, I would prefer the robot and hire experienced people to manage it.
16	For purely economic reasons, I would prioritize robots, but for other issues, a robot wouldn't replace a human.
17	I would prioritize robots and keep only the necessary people.
18	Robots because they are more efficient and competent.
19	I would prioritize people because I understand that there could be a union between humans and robots, but robots alone wouldn't be able to complete the work entirely.
20	I would replace everything possible with robots for repetitive tasks and would place people in roles requiring critical thinking.
21	If the robots are well-developed, they can work 24 hours a day, and the likelihood of errors is lower. The volume of work they can handle is higher than what a human can do, even though it's still necessary to have humans involved.
22	Functions can be performed by robots, saving money. However, it is necessary because humans possess critical thinking abilities that robots do not.
23	Only in functions that can be automated and provide a return, saving time for employees to perform other tasks.
24	I would prioritize robots because they would lead to more financial gains and select specialized individuals for the management and maintenance of the robots.
25	I would prioritize people by reallocating them to other tasks and investing in training so that these employees could perform activities requiring critical thinking, while I would keep robots for repetitive tasks.
26	If RPA was chosen to reduce costs and time, it doesn't make sense to prioritize or keep people in roles that RPA can perform. People are required people for evaluation and execution, especially in case of failures.
27	Economically, I would prefer to prioritize robots for tasks that can be automated and keep the necessary employees in other roles.
28	I would prioritize robots because I would want to save money on both salaries and other expenses. The fewer human errors, the greater the financial return for the organization, while people would be assigned to essential functions.
29	I would prioritize robots for tasks that are time-consuming for humans and keep employees engaged in activities that require human analysis and thinking.
30	I would prioritize robots for economic reasons, mitigating human error, and exponentially increasing the value added to my company. It would accomplish the same work while reducing costs related to human labor, including salaries, healthcare expenses, taxes, and saving time.
31	I would prioritize people, using robots for repetitive tasks and reallocating individuals. If the company's goal is to expand, there are always tasks for people to do. It's important to assess medium and long-term objectives, provide training for people who will be reallocated, and prepare them for this transition.

#	Q5 - Do you think RPA helps or replaces employees?
1	Depending on the company's objectives, it can either replace people or assist with the workload of others.
2	It helps as it reduces repetitive workload from employees
3	RPAs help people by handling the most tedious tasks at work and completing certain steps much faster than humans can.
4	It doesn't fully replace them, but it definitely helps them.
5	If an employee or a group of employees are only performing tasks that could be fully automated, the company has the choice to reassign the attributions of that employee or dismiss them, totally or partially.
6	They help workers by freeing up humans for more analytical and higher-value tasks in the company.
7	RPA is here to replace tedious and repetitive tasks that human has. It mimics human behavior without the human errors while the performance is also better.
8	If implemented correctly, it can increase employee satisfaction by allowing them to focus on tasks that generate more value. Therefore, RPA, along with a human touch, can be the key to a higher likelihood of process success.
9	If they are small, repetitive processes, it replaces tasks and not people, activities without the need for analysis.
10	RPA helps with the most repetitive parts, and people focus on what generates value.
11	It helps with replacements but also aids in maintaining tasks that couldn't be ensured because the number of hires decreases while tasks do not.
12	It helps humans with repetitive activities. It can free up those at the end of their careers for retirement, but the intention is to complement or free up for other activities.
13	It helps because people are still necessary; robots can generate errors that need to be corrected by human hands.
14	We can't claim that we're always helping or always replacing; it's usually a combination of both. It all depends on the perspective and how they are implemented.
15	It replaces, some RPAs can replace an entire department, and people are not always reallocated.
16	It helps more than it replaces, but in some cases, it does replace when the work is repetitive and doesn't require creativity and critical thinking, and there is no possibility of reallocation.
17	It helps because employees can move to more important roles.
18	In most cases, it helps people with significant roles rather than those with repetitive tasks.
19	It helps the employees because it optimizes time and reduces costs.
20	It helps the employees because it is essential for optimizing time and resources. People should be placed in non-repetitive areas and in critical areas that require human thinking.
21	Human knowledge about the process is essential, as is human intervention for development and maintenance.
22	They help; robots don't replace human analysis. However, people aren't always reassigned, it depends on the company's plan, and it can hinder the knowledge transfer for RPA development.
23	They help employees have more time to engage in more important activities.
24	It aids people by replacing repetitive tasks, requiring individuals to specialize in handling tasks that involve critical thinking.
25	It helps because it allows employees to focus on tasks that require critical thinking, while robots are used for more repetitive tasks.
26	Helps essential personnel and replace individuals in mechanical roles that don't require human reasoning because it doesn't always make sense to relocate these individuals to other functions.
27	It can replace tasks that can be fully automated and can assist individuals in roles requiring analytical thinking.
28	It helps with repetitive processes and replaces humans in functions where they are not necessary.
29	It helps employees by freeing them from repetitive tasks so they can focus on other things.
30	I believe RPA helps people by relieving them of a lot of repetitive tasks and replacing employees who are no longer needed.
31	It helps employees in repetitive activities.

#	Q6 - Do you believe that all individuals involved in the same project should have the same levels of permissions?
1	There should be project management, and accesses should be requested and granted based on each collaborator's responsibilities.
2	Security. A developer should not have access to financial records as it could be a breach in security
3	Each person should have the appropriate permissions for their role and the tasks they need to perform.
4	There are confidential and sensitive data that should only be accessed by whoever is needed.
5	Is important to protect business from data breaches or unauthorized changes.
6	There must be different permission levels due to data confidentiality issues and project vulnerabilities.
7	I believe they should have the level of permission of the job category they are currently performing to avoid confidentiality risks for example
8	Increased security, risk minimization, and role-based hierarchy are crucial as not all individuals require the same levels of access.
9	There are confidential data and each person's seniority to consider. Very junior employees don't need access to confidential information.
10	It should be segmented to eliminate risks.
11	They should be segmented according to functions, but there can be a person with access to everything.
12	Not everyone, needs to be a mix of experiences and responsibilities.
13	Having different levels of permissions and access rights can be a critical aspect of security and management.
14	I don't think all individuals on a project should have the same permissions, but there should be autonomy to fully carry out our work.
15	Should be a hierarchy; a junior should not have the same level as a senior who has a certain level of trust from the client.
16	Difficult to manage due to security reasons. Access should be based on each employee's responsibility.
17	There must be a hierarchy; people with more knowledge have higher levels of access.
18	No, for data security, access levels must be well-defined.
19	There are people with less knowledge than others, there needs to be a hierarchy.
20	There should be a hierarchy for direction; a junior doesn't reason like a senior and doesn't know the risks and processes. Knowledge is necessary for decision-making.
21	People may not always have access to all the information.
22	It's challenging to manage and analyze everything; however, it can hinder the speed and efficiency of the process.
23	Considering that processes involve confidential data, access should be limited according to the hierarchy.
24	People should only access what they need to know, limiting it to the area in which they specialize according to their responsibilities.
25	I believe so because it streamlines the work and eliminates the wait for permissions, always with supervision, regulation, and data encryption.
26	For security reasons, hierarchy must be respected to prevent errors, fraud, and other issues. People without sufficient knowledge and with high levels of permission can have a negative impact on the organization.
27	There are confidential pieces of information, and a certain level of trustworthiness is necessary to access and handle this type of information.
28	Because not everyone has the same perception and sensitivity regarding the systems and data used, they may end up making errors that could tarnish the organization's image, in addition to incurring costs and wasting time.
29	Because of the levels of responsibility, for example, a junior employee may not have as much knowledge about risks as a senior employee.
30	Because there should be an assignment of responsibility, and those who hold these responsibilities should be individuals whose roles in the project follow a hierarchy. Additionally, for security reasons, there should be a separation of functions and responsibilities.
31	For security reasons, and because not everyone applies knowledge in the same way, people should have permissions according to their responsibilities.

#	Q7 - In your opinion, is understanding and preparing employees important for reducing compliance risks in RPA?
1	The knowledge and ongoing training of employees are essential to prevent compliance risks such as regulatory violations, fraud, or data leaks.
2	It's always good to prepare employees to deal with anomalies that come from robotic processes, as they would more efficiently respond to what happened.
3	RPA is a simple technology; however, it can cause significant issues if those who use it lack basic knowledge of the process/technology.
4	If you are dealing with sensitive data, it is important that people are aware and know how to deal to avoid breaches.
5	Employees can have insights that helps identifying risks and addressing them before it escalates furthermore.
6	If workers were better informed about the reality of RPAs and even involved in their management, there would be fewer associated operational risks.
7	It is important in order to protect data integrity, data security, and employee and customer privacy
8	Training employees is a fundamental aspect of reducing compliance risks in RPA and data protection. There should be a culture of awareness and responsibility.
9	This should be part of the onboarding for each project, there should be a framework to understand the risk of actions.
10	It's important to be aware of the risks because sometimes tasks are carried out without awareness of the impact.
11	Training is very important; the structure of RPA, cross-modules, impacts, and risks should be explained.
12	It's very important because using robots for operations instead of humans, if there is any damage, it will be faster and on a larger scale.
13	Understanding and preparing employees is essential, so that they are aware of compliance, risks, and how to deal with them.
14	It's an important part of appropriate training according to roles, enabling preparation to face all difficulties, a very important factor in a company's growth.
15	Important are trainings, test environments, and permissions, as well as an employee to validate so that when there is an audit, an error is not considered fraud.
16	To mitigate risks, everyone should be aware. Sensitive data is used, and often, developers may not be aware of what type of data it is and how dangerous it can be.
17	Employees must be prepared because otherwise, the company is at risk due to poor preparation and understanding.
18	It's very important for employees to be more careful when developing and understand the impact it can have.
19	There should be a lot of awareness of the entire process; people need to understand what each permission can cause.
20	Everyone must be aware of the risks associated with the process and the tools to be used. Risks should be well understood, and it's very important to know what one is doing to avoid causing losses to the business.
21	It's necessary; people should understand the risks of their actions and the need as well.
22	It's essential, it's important to grasp the business, understand the technology being used, comprehend the access levels, and the purpose of each activity within the process.
23	So that employees understand and become more proactive in seeking solutions, thereby reducing risks.
24	Preparation is necessary; employees must understand what they are working on and the risks of their actions to the organization.
25	it's very important. It helps to better understand the business, avoiding future constraints, makes the work more direct, and regarding IT, it can even help developers feel more motivated by knowing what they are doing and the impact on people's daily lives.
26	Crucial to extract the best from the business and the process. If people are well-trained and comprehend what they are working on, the risks and real-life impact, the chances of errors occurring decrease.
27	The higher the level of knowledge, the lower the chance of making errors. People should be informed about the risks and benefits of what they are creating and handling.
28	I find it important both to avoid losses and to help and motivate each employee in their respective roles.
29	People need to understand the area they are working in, the real-life impact, and the risks.
30	Employees need to understand what they have access to, the information, and their responsibility to protect and handle that information as sensitive. They should also know how to handle this information to prevent data breaches.
31	It is necessary because an individual may not know the entire context, but they should understand the risks that execution can bring, including impacts on the company such as a bad reputation and significant losses.

CHAPTER 7

Conclusions

This concluding chapter offers a comprehensive synthesis of the key findings presented in this thesis, structured into four main sections. The first and most extensive section, the summary and discussion, explores the essential outcomes of the research articles generated throughout this thesis, providing a comprehensive analysis of the results derived from testing the proposed conceptual framework. The concluding remarks furnish critical insights and contributions, illustrating how both scholars and practitioners can leverage these findings. The section on limitations acknowledges the constraints and challenges encountered during the research, addressing the scope of the study, the rapid evolution of technology, cultural influences, and the integration of automation technologies within business continuity frameworks, which may affect the applicability and scalability of the findings across different organizational and cultural settings. Lastly, the future work section highlights promising ways for further investigation and research, building upon the foundation established by this thesis.

7.1. Summary and Discussion

This thesis studies the integration of RPA and IPA into BC frameworks. It underscores the importance of aligning these automation technologies with GRC structures to ensure operational resilience and effectiveness. Through a comprehensive analysis, the thesis explores the intersection of RPA/IPA with standards like IEEE 2755:2020 and ISO 22301:2019, demonstrating how automation can enhance business continuity strategies while navigating the complexities of governance, security, risk, and compliance.

The research covers the impact of automation on auditing, focusing on the unique challenges faced by the financial sector. Additionally, it explores the risks that RPA and IPA can introduce into business operations and provides insights into mitigating these risks through robust frameworks. The study also examines the role of governance and human capital in effectively managing the transition to automation. By exploring these themes, the thesis contributes significantly to understanding how organizations can harness automation technologies to enhance business continuity while maintaining operational efficiency and resilience.

The findings of this thesis reveal that RPA and IPA offer substantial opportunities to streamline business processes and enhance operational resilience, provided that their integration is managed within a comprehensive framework. A strategic approach to implementing RPA and IPA technologies is crucial, aligning them with BC strategies to harness their full potential while mitigating the inherent risks.

Governance

Governance plays a pivotal role in guiding the implementation of automation, ensuring that clear policies, risk management practices, and compliance standards are in place. Effective governance frameworks ensure that automation initiatives align with an organization's broader objectives while adhering to industry standards and regulatory requirements. By establishing clear guidelines for the deployment and management of RPA and IPA, organizations can avoid pitfalls such as inefficiencies, security vulnerabilities, and non-compliance, which can arise from inadequate oversight.

Risk Management and Compliance

The research emphasizes the importance of security and compliance, particularly in sectors like finance, where automation is reshaping traditional auditing practices. As automation increases the organization's exposure to cyber threats and compliance risks, it is imperative to implement risk management frameworks that anticipate and address these vulnerabilities. Compliance with industry standards like IEEE 2755.2:2020 and ISO 22301:2019 helps organizations navigate the complex regulatory landscape, ensuring that automated processes are secure and aligned with legal requirements. Failing to adhere to these standards can result in costly penalties, reputational damage, and disruptions to business continuity.

Risk Impacts and Business Continuity Planning

The analysis of risk impacts reveals that organizations need to update their BC plans to account for the new dependencies and vulnerabilities that automation introduces. RPA and IPA change the nature of dependencies in workflows, potentially creating new points of failure that must be addressed in BC strategies. A proactive approach to risk management, involving the identification of potential disruptions and the implementation of contingencies, is crucial to ensure that organizations can swiftly recover from automation failures. Automated processes should be designed with redundancies and fail-safes to prevent a single point of failure from causing widespread operational disruption.

Human Capital and Change Management

The thesis also highlights the human capital challenges associated with automation, emphasizing the need for organizations to manage the transition effectively. Automation introduces changes that can redefine roles and responsibilities, necessitating change management strategies and workforce training. Employees need to be equipped with the skills required to work alongside automated systems, and resistance to change must be managed to avoid undermining the effectiveness of automation initiatives. By fostering a culture that

embraces change and continuous learning, organizations can better integrate RPA and IPA technologies into their operations.

Audit and Automation

Another important aspect highlighted is the impact of automation on auditing practices. As financial institutions increasingly adopt RPA and IPA, there is a need to redefine traditional auditing practices to address the complexities introduced by automation. Automated processes require rigorous auditing to ensure compliance and to detect any anomalies that could indicate fraud or operational issues. This thesis provides insights into how organizations can evolve their auditing frameworks to meet the demands of the automated era.

In conclusion, this thesis provides valuable insights into the integration of RPA and IPA into business continuity frameworks. By aligning automation initiatives with standards, governance structures, and BC objectives, organizations can harness the benefits of automation while maintaining operational resilience and compliance. The research emphasizes the need for a holistic approach that integrates technology with governance, risk management, compliance, and change management to ensure that RPA and IPA deliver their intended benefits without compromising the organization's ability to respond to disruptions effectively.

7.2. Final Remarks

From a practical perspective, the integration of RPA and IPA into BC frameworks is most effective when individuals within the organization understand and actively engage with the governance structures guiding these technologies. This understanding emerges when individuals recognize that automation is implemented through a well-structured system of policies and best practices, which they are encouraged to utilize to enhance organizational resilience. By effectively aligning RPA and IPA initiatives with robust GRC frameworks, organizations can create an environment that fosters ownership, responsibility, and commitment among employees. Leaders play a crucial role in cultivating this culture of trust and responsibility, ensuring that employees have the resources and support needed to effectively manage automated workflows and maintain business continuity.

As a result of this thesis, organizations aiming to promote positive behaviours among their employees, such as taking ownership of automated processes, participating in governance frameworks, and ensuring continuity in operations, can benefit in two significant ways. First, they can work towards refining their governance frameworks to align more closely with automation technologies. This involves developing policies, training programs, and communication channels that support automation goals, thus creating an environment where

employees recognize the value and effectiveness of RPA and IPA mechanisms, leading to improved business continuity. Second, organizations can foster a culture of trust, open communication, and collaboration by encouraging creativity and innovation, rewarding employees for effectively managing automated processes, and promoting a shared sense of responsibility for business continuity.

In sum, the findings of this thesis underscore the importance of aligning GRC frameworks with automation technologies to enhance business continuity. By fostering a culture of awareness and responsibility at the management level, organizations can improve their governance structures and ensure that employees actively contribute to automation strategies, ultimately enhancing operational resilience.

This thesis contributes significantly to the body of knowledge on RPA, IPA, and BC management. It bridges the gap between automation technologies and business continuity by exploring the previously under-researched intersection of automation and BC. Moreover, it considers governance and risk management as critical factors in managing automation, with an emphasis on international standards that guide these practices. While prior research on RPA and IPA has primarily focused on efficiency improvements, this thesis provides new insights by demonstrating how these technologies can be aligned with BC strategies to improve organizational resilience. Finally, this thesis highlights the importance of integrating automation with governance and risk management to align IT strategies with business objectives and enhance organizational effectiveness.

7.3. Limitations

While this research provides valuable insights, it is important to acknowledge its limitations. The scope of the current study is confined to the specific contexts in which the automation technologies were tested, which may not accurately reflect all organizational or industrial environments. Additionally, the rapid evolution of technology could quickly outpace the frameworks and strategies suggested, necessitating continual updates and reassessment of the proposed solutions.

Moreover, the impact of cultural differences on the adoption and effectiveness of automation technologies remains underexplored and could significantly affect the generalizability of the findings. This is particularly relevant as automation technologies are deployed across diverse global settings, where cultural variables can influence both the implementation and outcomes of such technologies.

Detailed investigations into specific risks associated with newer automation technologies, especially in sensitive industries, remain sparse. Additionally, the psychological impacts of

automation on employees and resistance to change are not comprehensively covered, indicating a gap in understanding the full spectrum of human capital management in automated environments.

Furthermore, the integration of these technologies within business continuity plans is not fully explored, particularly the long-term impacts on organizational resilience during disruptions. The research on how automated systems can be designed to be robust enough to support business continuity during crises is still developing.

Future research should address these limitations by expanding the variety of test environments, developing specific methodologies for advanced automated systems, and updating strategies in line with technological advancements. Studies should also consider the psychological and cultural impacts more comprehensively to enhance the adaptability and effectiveness of automation technologies across different global contexts. Additionally, further exploration into how automation can be embedded into business continuity frameworks to ensure operational resilience under various scenarios would be beneficial. This includes assessing the effectiveness of automated processes in real crises and refining business continuity strategies accordingly.

7.4. Future Work

The future work outlined emphasizes the need for continued research in several critical areas. Expanding automation frameworks to meet diverse industry requirements, developing specialized risk management strategies, and understanding the impact on human capital more in-depth are essential next steps in understanding in more detail the integration of automation into BCM. Moreover, examining the evolving role of auditing and compliance in an automated context will further refine our understanding of how automation influences business processes. By addressing these areas, future research will significantly enhance our understanding of RPA and IPA in organizational contexts:

1. **Expanding Frameworks for Automation Integration:**

   One of the areas ripe for future exploration is the expansion of existing frameworks that guide the integration of RPA and IPA into BCM. By conducting further research into how these frameworks can be enhanced and adapted for different industries and organizational contexts, future studies can provide more comprehensive guidelines that cater to diverse needs. This includes tailoring frameworks for sectors with specific regulatory and operational requirements, such as healthcare or finance, and examining how industry-specific regulations interact with automation technology.

2. **Risk Management Strategies in Automated Environments:**

Future research should delve deeper into developing effective risk management strategies that are specifically tailored to automated environments. Understanding the nuances of new risks introduced by RPA and IPA technologies and how these interact with existing BC plans is crucial. Studies can explore risk mitigation techniques, from process redundancies to cybersecurity measures, that organizations can employ to safeguard their operations in an increasingly automated landscape.

3. **Human Capital and Organizational Change Management:**

   A significant aspect of integrating automation into business processes involves managing the impact on human capital. Future work should focus on the change management strategies required to facilitate the transition of the workforce into an automated environment. This involves exploring ways to upskill employees, address resistance to change, and ensure seamless integration of human and automated workflows.

4. **Auditing and Compliance in Automated Systems:**

   The evolving role of auditing in the age of automation is another area requiring further exploration. Research can focus on developing new methodologies for auditing automated systems to ensure compliance with internal policies and external regulations. This involves examining how auditors can leverage automation for improved auditing processes and how new auditing frameworks can be developed for an automated environment.

References

[1] A. Margherita, M. Nasiri, and T. Papadopoulos, “The application of digital technologies in company responses to COVID-19: an integrative framework,” *Technol Anal Strateg Manag*, vol. 0, no. 0, pp. 1–14, 2021, doi: 10.1080/09537325.2021.1990255.

[2] T. Papadopoulos, K. N. Baltas, and M. E. Balta, “The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice,” *Int J Inf Manage*, vol. 55, no. July, p. 102192, 2020, doi: 10.1016/j.ijinfomgt.2020.102192.

[3] A. S. Butt, “Mitigating the effects of COVID-19: an exploratory case study of the countermeasures taken by the manufacturing industry,” *Journal of Business and Industrial Marketing*, vol. ahead-of-print, no. August, 2021, doi: 10.1108/JBIM-04-2021-0236.

[4] M. Röglinger *et al.*, “Exogenous Shocks and Business Process Management: A Scholars’ Perspective on Challenges and Opportunities,” *Business and Information Systems Engineering*, vol. 64, no. 5, pp. 669–687, 2022, doi: 10.1007/s12599-021-00740-w.

[5] D. António *et al.*, “Engineering Management in Production and Services Robotic Process Automation (RPA) adoption: a systematic literature review,” 2022, doi: 10.2478/emj-2022-0012.

[6] “2755-2017 - IEEE Guide for Terms and Concepts in Intelligent Process Automation | IEEE Standard | IEEE Xplore.” Accessed: Apr. 07, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/8070671

[7] J. C. Brás, R. F. Pereira, S. Moro, I. S. Bianchi, and R. Ribeiro, “Understanding how Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019,” *IEEE Access*, pp. 1–1, 2023, doi: 10.1109/ACCESS.2023.3337159.

[8] J. Brás, R. Pereira, and S. Moro, “Intelligent Process Automation and Business Continuity: Areas for Future Research,” *Information 2023, Vol. 14, Page 122*, vol. 14, no. 2, p. 122, Feb. 2023, doi: 10.3390/INFO14020122.

[9] J. von Solms and J. Langerman, *Risks_and_Threats_Arising_from_the_Adoption of_Digital_Technology_in_Treasury*, vol. 1339. Springer International Publishing, 2020. doi: 10.1007/978-3-030-66039-0_1.

[10] N. Joshi, “Leverage RPA, But Plan For Its Inherent Risks, Too!” Accessed: Jan. 09, 2023. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/06/28/leverage-rpa-but-plan-for-its-inherent-risks-too/?sh=58aebc2a11d1

[11] KPMG, “Managing risks of the growing RPA jungle,” p. 14, 2018, [Online]. Available: https://assets.kpmg/content/dam/kpmg/in/pdf/2018/12/Managing-risks-the-growing-RPA-jungle.pdf

[12] R. Namchoochai, S. Kiattisin, S. Darakorn Na Ayuthaya, and S. Arunthari, “Elimination of FinTech Risks to Achieve Sustainable Quality Improvement,” *Wirel Pers Commun*, vol. 115, no. 4, pp. 3199–3214, 2020, doi: 10.1007/s11277-020-07201-9.

[13] M. Gotthardt, D. Koivulaakso, O. Paksoy, C. Saramo, M. Martikainen, and O. Lehner, “ACRN Journal of Finance and Risk Perspectives Current State and Challenges in the Implementation of Smart Robotic Process Automation in Accounting and Auditing,” *ACRN Journal of Finance and Risk Perspectives*, vol. 9, pp. 90–102, 2020, doi: 10.35944/jofrp.2020.9.1.007.

[14] E. Candratio, M. P. Harita, A. D. Hartanto, and M. S. Hermawan, “Adoption of Robotic Process Automation in External Auditing Process in Metropolitan Indonesia: A Qualitative Approach,” *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 10, no. 2, pp. 21–28, Jun. 2023, doi: 10.35957/JATISI.V10I2.4323.

[15] T. Nunes, J. Leite, and I. Pedrosa, “Intelligent Process Automation: An Overview over the Future of Auditing,” *Iberian Conference on Information Systems and Technologies, CISTI*, vol. 2020-June, Jun. 2020, doi: 10.23919/CISTI49556.2020.9140969.

[16] J. Asef-Sargent, A. C. Lewis, K. E. Everson, and J. C. Steinhoff, “Put on Your Auditor Hat to Help Avoid Turbulence on the Intelligent Automation Journey!,” *Journal of Government Financial Management*, vol. 68, no. 4, pp. 18–25, 2020, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=141939720&site=eds-live

[17] D. Kahan, A. Oltmanns, G. Kaczmarskyj, C. Lamberton, and A. Gillard, “Risk and control considerations within robotic process automation implementations Balancing transformation with risk Addressing history before it repeats itself,” p. 12, 2018, [Online]. Available: https://engineering.report/Resources/Whitepapers/bceab695-0ac9-430c-ae6c-2fe8a4daa925_Risk-control-considerations-within-robotic-process-automation-implementations.pdf

[18] N. Jain, “The risk of RPA implementation and how to mitigate it.” Accessed: Mar. 20, 2023. [Online]. Available: https://www.capgemini.com/2020/09/the-risk-of-rpa-implementation-and-how-to-mitigate-it/

[19] Hugo Ciopages, “Robotic Process Automation: The opportunity, risks and rewards.” Accessed: Jun. 04, 2023. [Online]. Available: https://www.ciopages.com/robotic-process-automation/

[20] A. K. Jallow, B. Majeed, K. Vergidis, A. Tiwari, and R. Roy, “Operational risk analysis in business processes,” *BT Technology Journal*, vol. 25, no. 1, pp. 168–177, 2007, doi: 10.1007/s10550-007-0018-4.

[21] C. Hutchins, “Robotic Process Automation (RPA): Use Cases And Risks To Consider.” Accessed: Jun. 17, 2023. [Online]. Available: https://www.cioapplications.com/cxoinsights/robotic-process-automation-rpa-use-cases-and-risks-to-consider-nid-4073.html

[22] F. Fukuyama, “Governance: What Do We Know, and How Do We Know It?,” *Annual Review of Political Science*, vol. 19, pp. 89–105, 2016, doi: 10.1146/annurev-polisci-042214-044240.

[23] ISACA, *Governance and Management Objectives*. 2018. [Online]. Available: https://www.isaca.org/resources/cobit

[24] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, “Information security governance challenges and critical success factors: Systematic review,” *Comput Secur*, vol. 99, p. 102030, 2020, doi: 10.1016/j.cose.2020.102030.

[25] D. Kedziora and E. Penttinen, “Governance models for robotic process automation: The case of Nordea Bank:,” *https://doi.org/10.1177/2043886920937022*, vol. 11, no. 1, pp. 20–29, Jul. 2020, doi: 10.1177/2043886920937022.

[26] M. Chapple, J. M. Stewart, and D. Gibson, “Security Governance Through Principles and Policies,” *CISSP, Eighth Edition*, pp. 1–48, 2018, doi: 10.1002/9781119549567.ch1.

[27] C.-C. Osman, “Robotic Process Automation: Lessons Learned from Case Studies”, doi: 10.12948/issn14531305/23.4.2019.06.

[28] N. Rizun, A. Revina, and V. G. Meister, “Assessing business process complexity based on textual data: Evidence from ITIL IT ticket processing,” *Business Process Management Journal*, vol. 27, no. 7, pp. 1966–1998, 2021, doi: 10.1108/BPMJ-04-2021-0217.

[29] R. Alt, “Managing AI is managing complexity - An interview with Rahul C. Basole,” *Electronic Markets*, pp. 1119–1125, 2022, doi: 10.1007/s12525-022-00585-5.

[30] K. Ng, C. Chen, C. Lee, … J. J.-A. E., and undefined 2021, “A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives,” *Elsevier*, 2021, doi: 10.1016/j.aei.2021.101246.

[31] A. Azadegan, M. M. Parast, L. Lucianetti, R. Nishant, and J. Blackhurst, “Supply Chain Disruptions and Business Continuity: An Empirical Assessment,” 2020.

[32] N. Russo, H. S. Mamede, L. Reis, J. Martins, and F. Branco, “Exploring a Multidisciplinary Assessment of Organisational Maturity in Business Continuity: A Perspective and Future Research Outlook,” *Applied Sciences 2023, Vol. 13, Page 11846*, vol. 13, no. 21, p. 11846, Oct. 2023, doi: 10.3390/APP132111846.

[33] D. da Silva Costa, H. São Mamede, and M. Mira da Silva, “Robotic Process Automation (RPA) Adoption: A Systematic Literature Review,” 2021. doi: 10.2478/emj-2022-0012.

[34] H. Lei, X. Fang, T. M. Rajkumar, and C. Holsapple, “Recovering Troubled IT Projects: The Roles of Transformational Leadership and Project Complexity,” *Information Systems Frontiers*, vol. 24, no. 1, pp. 233–245, 2022, doi: 10.1007/s10796-020-10068-7.

[35] E. Zio, “The future of risk assessment,” *Reliab Eng Syst Saf*, vol. 177, no. April, pp. 176–190, 2018, doi: 10.1016/j.ress.2018.04.020.

[36] M. Lacity and L. Willcocks, *Robotic Process Automation and Risk Mitigation: The Definitive Guide*. SB Publishing, 2017. [Online]. Available: https://books.google.es/books/about/Robotic_Process_Automation_and_Risk_Miti.html?id=bvkJtAEACAAJ&redir_esc=y

[37] G. Priyadarshi, “Inherent Risk in Adopting RPA and Opportunities for Internal,” *ISACA Journal*, vol. 6, pp. 50–52, 2019, [Online]. Available: https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwidqvrWnK6GAxUTD6IDHY0fAQ4YABAAGgJsZQ&ase=2&gclid=Cj0KCQjw3tCyBhDBARIsAEY0XNmEpr2SYJtmEZYdbU87T7WtWPR2G1RUnAVlGo5s8ynWAhOxG3f153AaApEqEALw_wcB&ohost=www.google.com&cid=CAESVOD241tL20WgnT5BtiziaMyJeS2Ui1uRLjSiciNjiaLzhZsklzS-9rbUUKo1bsTLLEi5y4hz7SFVjXg0b3wcy8YfXy_6aBuJhKiFB3XN_NZzxQ8N6g&sig=AOD64_2AuHtpU9UxzrYeIUaQot8zpHbD5Q&q&nis=4&adurl&ved=2ahUKEwjvqPPWnK6GAxVPKRAIHUfyC0AQ0Qx6BAgGEAE

[38] D. Ahern, “Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon,” *European Business Organization Law Review*, vol. 22, no. 3, pp. 395–432, 2021, doi: 10.1007/s40804-021-00217-z.

[39] D. J. Lewis and J. F. McCallum, “Utilizing Advanced Technologies to Augment Pharmacovigilance Systems: Challenges and Opportunities,” *Ther Innov Regul Sci*, vol. 54, no. 4, pp. 888–899, 2020, doi: 10.1007/s43441-019-00023-3.

[40] G. Pavlidis, “Europe in the digital age: regulating digital finance without suffocating innovation,” *Law,_Innovation_and_Technology*, vol. 13, no. 2, pp. 464–477, 2021, doi: 10.1080/17579961.2021.1977222.

[41] P. Leslie Willcocks and A. Craig, “The Outsourcing Unit Working Research Paper Series The IT Function and Robotic Process Automation Research on Business Services Automation Research Objective,” 2015, Accessed: Apr. 23, 2024. [Online]. Available: www.lse.ac.uk/management/research/outsourcingunit

[42] L. Van der Walt and S. Van Coller-Peter, “Coaching for development of leaders’ awareness of integrity: An evidence-based approach,” *South African Journal of Business Management*, vol. 51, no. 1, pp. 1–10, 2020, doi: 10.4102/SAJBM.V51I1.1943.

[43] B. Unhelkar and T. Gonsalves, “Enhancing Artificial Intelligence Decision Making Frameworks to Support Leadership During Business Disruptions,” *IT Prof*, vol. 22, no. 6, pp. 59–66, 2020, doi: 10.1109/mitp.2020.3031312.

[44] B. Herbane, “Rethinking organizational resilience and strategic renewal in SMEs,” *Entrepreneurship and Regional Development*, vol. 31, no. 5–6, pp. 476–495, 2019, doi: 10.1080/08985626.2018.1541594.

[45] L. Willcocks, M. Lacity, and A. Craig, “Robotic process automation: Strategic transformation lever for global business services?,” *Journal of Information Technology Teaching Cases*, vol. 7, no. 1, pp. 17–28, 2017, doi: 10.1057/s41266-016-0016-9.

[46] G. Parise, L. Martirano, and L. Parise, “‘Energy castles’ equalized to strategic structures for disaster recovery in emergency,” *2017 IEEE Industry Applications Society Annual Meeting, IAS 2017*, vol. 2017-Janua, pp. 1–6, 2017, doi: 10.1109/IAS.2017.8101874.

[47] “2755.2-2020 - IEEE Recommended Practice for Implementation and Management Methodology for Software-Based Intelligent Process Automation | IEEE Standard | IEEE Xplore.” Accessed: Apr. 07, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9404959

[48] ISO, “ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements,” 2019 Accessed: Dec. 26, 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

[49] IEEE, “IEEE Guide for Terms and Concepts in Intelligent Process Automation,” *IEEE_Std_2755-2017*, pp. 1–16, 2017, doi: DOI: 10.1109/IEEESTD.2017.8070671.

[50] “2755.1-2019 - IEEE Guide for Taxonomy for Intelligent Process Automation Product Features and Functionality | IEEE Standard | IEEE Xplore.” Accessed: Feb. 11, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/8764094/citations?tabFilter=papers#citations

[51] S. Brás, José; Guerreiro, “Challenges for Assessing and Designing Business Continuity Processes,” 2016, [Online]. Available: http://eprints.fri.uni-lj.si/3341/1/Radar-proceedings.pdf

[52] A. Van Looy, “Innovating Organizational Processes with New Technologies: Problems and Solutions,” *IT Prof*, vol. 22, no. 5, pp. 71–80, 2020, doi: 10.1109/MITP.2020.2969614.

[53] R. Uskenbayeva, Z. Kalpeyeva, R. Satybaldiyeva, A. Moldagulova, and A. Kassymova, “Applying of RPA in Administrative Processes of Public Administration,” *Proceedings - 21st IEEE*

Conference on Business Informatics, CBI 2019, vol. 2, pp. 9–12, 2019, doi: 10.1109/CBI.2019.10089.

[54] J. Bras, "Bootstrapping enterprise models with business continuity processes and DEMO," 2017, [Online]. Available: https://recil.ensinolusofona.pt/bitstream/10437/8385/1/Tese_Jos%C3%A9_Cascais_Br%C3%A1s_MEISI_2017.pdf

[55] H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," *IET Cyber-Physical Systems: Theory and Applications*, vol. 4, no. 4, pp. 332–340, 2019, doi: 10.1049/iet-cps.2018.5079.

[56] R. Mahanti, *Data Governance and Data Management: Contextualizing Data Governance Drivers, Technologies, and Tools*. 2021. [Online]. Available: https://link.springer.com/book/10.1007/978-981-16-3583-0

[57] G. Georgiadis and G. Poels, *Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study*, vol. 19, no. 1. Springer Berlin Heidelberg, 2021. doi: 10.1007/s10257-020-00500-5.

[58] "ISO 22313:2020(en), Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301." Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-2:v1:en

[59] T. Drewitt, "A Manager's Guide to ISO22301 A practical guide to developing and implementing a business continuity management system," 2013, Accessed: Feb. 18, 2023. [Online]. Available: www.itgovernance.co.uk

[60] "ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements." Accessed: Apr. 02, 2023. [Online]. Available: https://www.iso.org/standard/82875.html

[61] "Legal requirements, ISO standards, and best practice for business continuity management | Protective Security Requirements." Accessed: Apr. 02, 2023. [Online]. Available: https://protectivesecurity.govt.nz/governance/business-continuity-management/legal-requirements-iso-standards-and-best-practice-for-business-continuity-management/

[62] "Moving from BS 25999-2 to ISO 22301." Accessed: Apr. 04, 2023. [Online]. Available: https://www.bsigroup.com/documents/iso-22301/resources/bsi-bs25999-to-iso22301-transition-uk-en.pdf

[63] BSI, "ISO 22301 Business Continuity Plan | BSI." Accessed: Apr. 02, 2023. [Online]. Available: https://www.bsigroup.com/en-ID/ISO-22301/

[64] "ISO 22301, The Business Continuity Management Standard," *https://www.isms.online/*, Accessed: Apr. 02, 2023. [Online]. Available: https://www.isms.online/iso-22301/

[65] "NQA ISO 22301 Implementation Guide." Accessed: Feb. 18, 2023. [Online]. Available: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-22301-Implementation-Guide.pdf

[66] J. C. Brás, R. F. Pereira, M. Fonseca, R. Ribeiro, and I. S. Bianchi, “Advances in Auditing and Business Continuity: A Study in Financial Companies,” *Journal of Open Innovation: Technology, Market, and Complexity*, p. 100304, May 2024, doi: 10.1016/J.JOITMC.2024.100304.